RSA NETWITNESS® PLATFORM

Leitfaden zum Ereignisquellenmanagement

für Version 11.2

Kontaktinformationen

RSA Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

Dell ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2019

Inhalt

Informationen über Ereignisquellenmanagement

Mit dem Modul „Ereignisquelle“ in NetWitness Platform erhalten Sie eine einfache Methode, um Ereignisquellen zu managen und Warnmeldungsrichtlinien für die Ereignisquellen zu konfigurieren.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Verwaltung von Ereignisquellen und die Konfiguration ihrer Überwachung. Er zeigt auch, an welcher Stelle im Prozess die Konfiguration von Alarmen und Warnmeldungseinstellungen angeordnet ist.

Voraussetzungen

Es gibt zwei Berechtigungen in Bezug auf Ereignisquellenmanagement:

- **Ereignisquellen anzeigen** ist für die Benutzer erforderlich, um Ereignisquellen und deren Attribute, Schwellenwerte und Richtlinien anzuzeigen.
- **Ereignisquellen ändern** ermöglicht den Benutzern, Ereignisquellen hinzuzufügen, zu bearbeiten und anderweitig zu aktualisieren.

Weitere Details finden Sie in den folgenden Themen:

- Im Thema *Registerkarte „Rollen“*, verfügbar im Handbuch **Systemsicherheit und Benutzerverwaltung** > **Referenzen** > **Ansicht „Administration > Sicherheit** > **Registerkarte „Rollen“**.
- Im Thema *Rollenberechtigungen* werden die integrierten NetWitness Platform-Systemrollen beschrieben, die den Zugriff auf die Benutzeroberfläche steuern. Verfügbar im Handbuch **Systemsicherheit und Benutzerverwaltung** > **So funktioniert Role-Based Access Control**.
- Im Thema *Managen von Benutzern mit Rollen und Berechtigungen* wird beschrieben, wie Sie in NetWitness Platform mithilfe von Rollen und Berechtigungen Benutzer managen. Verfügbar im Handbuch **Systemsicherheit und Benutzerverwaltung** > **Managen von Benutzern mit Rollen und Berechtigungen**.

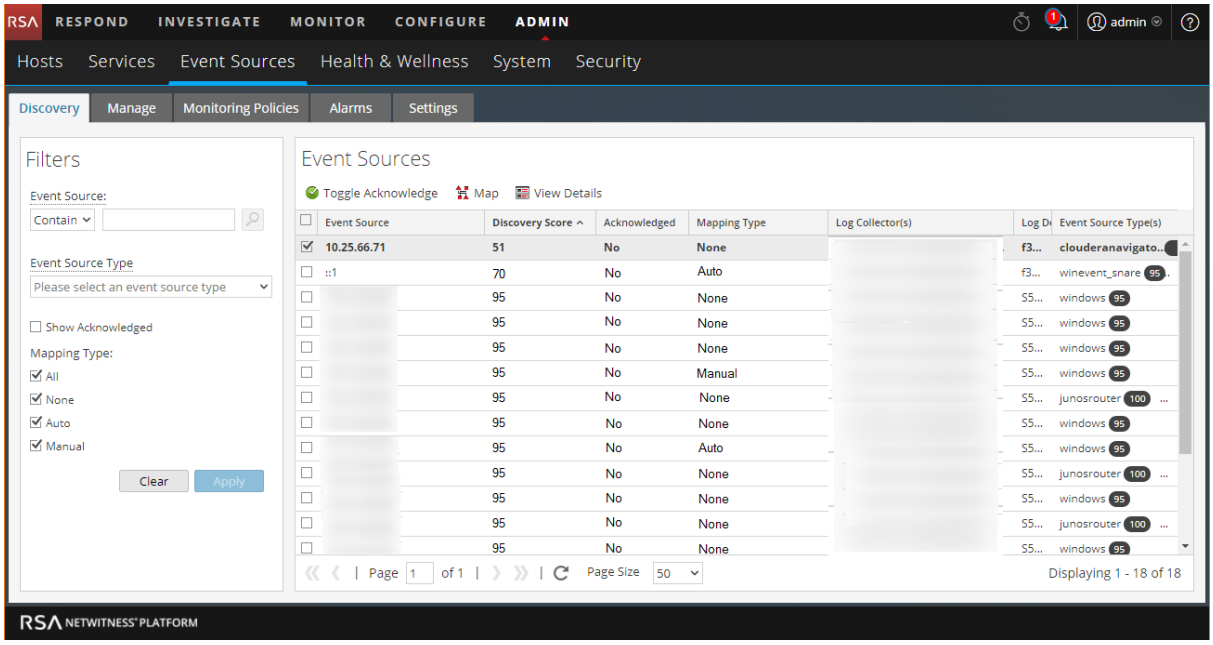
AutomatischeZuordnung?

Seit der Einführung von RSA NetWitness® Platform Version 11.1 ordnet das System eingehende Ereignisse automatisch anhand früherer Protokolle, die von dieser Adresse erhalten wurden, einem Typ zu und reduziert damit die Anzahl der Elemente, für die Ihre Aufmerksamkeit im Erkennungsworkflow erforderlich ist. Die Benutzeroberfläche gibt an, dass eine Adresse im Erkennungsworkflow automatisch zugeordnet wurde.

Navigieren Sie zu „Ereignisquellenmanagement“.

Führen Sie die folgenden Schritte aus, um Details zu den vorhandenen Ereignisquellengruppen anzuzeigen:

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.



2. Klicken Sie auf eine der folgenden Optionen:

- Die Registerkarte **Discovery**. Verwenden Sie diese Registerkarte, um die Ereignisquellentypen einzusehen, die NetWitness für jede Adresse ermittelt hat, und die Zuverlässigkeit des Systems hinsichtlich der Wahrscheinlichkeit, dass sie vollständig korrekt identifiziert wurden.
- Registerkarte **Managen**: Auf dieser Registerkarte können Sie Ereignisquellengruppen hinzufügen, bearbeiten und löschen sowie Details für Ihre bestehenden Ereignisquellengruppen anzeigen.
- Registerkarte **Überwachungsrichtlinien**: Auf dieser Registerkarte können Sie die Warnmeldungskonfigurationen für die Ereignisquellen anzeigen oder bearbeiten.
- Die Registerkarte **Alarme**. Verwenden Sie diese Registerkarte, um die Details der Alarme anzuzeigen, die erzeugt wurden. Alarme werden erzeugt, wenn Ereignisquellen ihre festgelegten Schwellenwerte über- oder unterschreiten.
- Registerkarte **Einstellungen**. Verwenden Sie diese Registerkarte, um das Verhalten für automatische Warnmeldungen anzuzeigen oder zu ändern.
- Die Registerkarte **Protokoll-Parser-Regeln**. Auf dieser Registerkarte können Sie Protokoll-Parser-Regeln anzeigen und erkennen, wie diese Regeln bestimmte Protokolle analysieren.

Hinweis: Wenn das System Protokolle von einer Ereignisquelle empfängt, die derzeit nicht in der Ereignisquellenliste vorhanden ist, fügt NetWitness Platform die Ereignisquelle automatisch zur Liste hinzu. Wenn die Ereignisquelle den Kriterien für eine beliebige vorhandene Gruppe entspricht, wird sie außerdem Teil dieser Gruppe.

Funktionsweise von Alarmen und Benachrichtigungen

Das Modul „Ereignisquelle“ in NetWitness Platform zeigt Alarme an und sendet Benachrichtigungen basierend auf Alarmen, die ausgelöst werden.

Für Alarme ist Folgendes zu beachten:

Es gibt zwei Arten von Alarmen: **automatische** (ausgelöst, wenn Baselines überschritten oder nicht erfüllt sind) und **manuelle** (konfiguriert mithilfe von Schwellenwerten).

- **Automatisch**: Wenn Sie automatische Warnmeldungen einschalten, meldet das System Alarme für **alle** Ereignisquellen, die über oder unter ihre normalen Baselines um das erforderliche Maß hinausgehen. Sie können den „über/unter“-Prozentsatz auf der Registerkarte Registerkarte „Einstellungen“ angeben.
- **Manuell**: Das System warnt immer dann, wenn eine Ereignisquelle die Schwellenwerte in der Richtlinie für die assoziierten Gruppen überschreitet.
- Alarme werden auf der Benutzeroberfläche auf der Registerkarte Registerkarte „Alarme“ angezeigt.

Für Benachrichtigungen ist Folgendes zu beachten:

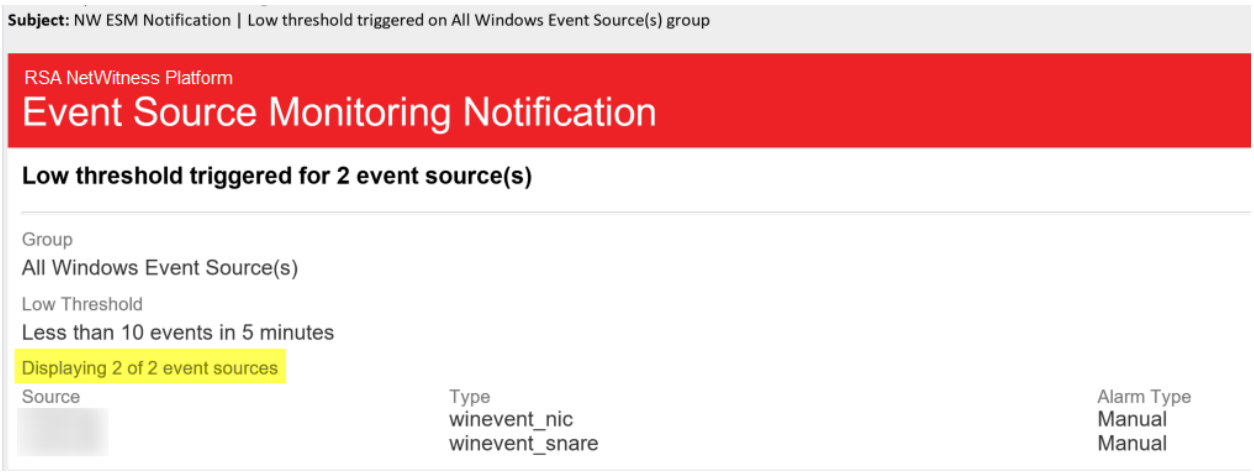
- So erhalten Sie manuelle Benachrichtigungen (per e-Mail, SNMP oder Syslog):
  - Geben Sie eine Policy für eine Ereignisquellengruppe an.
  - Legen Sie einen hohen oder niedrigen Schwellenwert (oder beide) fest.
  - Aktivieren Sie die Policy.
- So erhalten Sie automatische (Baseline-) Benachrichtigungen:
  - „Baseline-Warnmeldungen“ muss aktiviert sein. Es ist standardmäßig aktiviert.
  - Sie müssen „Benachrichtigungen von der automatischen Überwachung“ aktivieren. Weitere Informationen finden Sie unter Konfigurieren von automatischen Warnmeldungen.
  - Die Ereignisquelle, die den Alarm auslöst, muss in einer Gruppe sein, die eine Policy aktiviert hat.
- Wenn Sie automatische Warnmeldungen eingeschaltet haben und Sie eine Policy und einen Schwellenwert für eine Gruppe konfiguriert haben:
  - Wenn die Ereignisquelle über ihre Baseline hinausgeht, wird Ihnen eine automatische Warnmeldung angezeigt und Sie erhalten eine Benachrichtigung.
  - Wenn die Ereignisquelle über ihre Schwellenwerte hinausgeht, wird Ihnen eine manuelle Warnmeldung angezeigt und Sie erhalten eine Benachrichtigung.
  - Wenn beides geschieht (Schwellenwert und Baseline werden überschritten oder nicht erfüllt), erhalten Sie zwei Alarme (sichtbar auf der Registerkarte „Alarme“) und eine Benachrichtigung, die beide Alarme anzeigt. Diese Benachrichtigung wird die Ereignisquelle auflisten, die zweimal doppelt alarmiert hat. Dabei gibt ein Punkt auf der Liste an, dass es ein automatischer Alarm war.

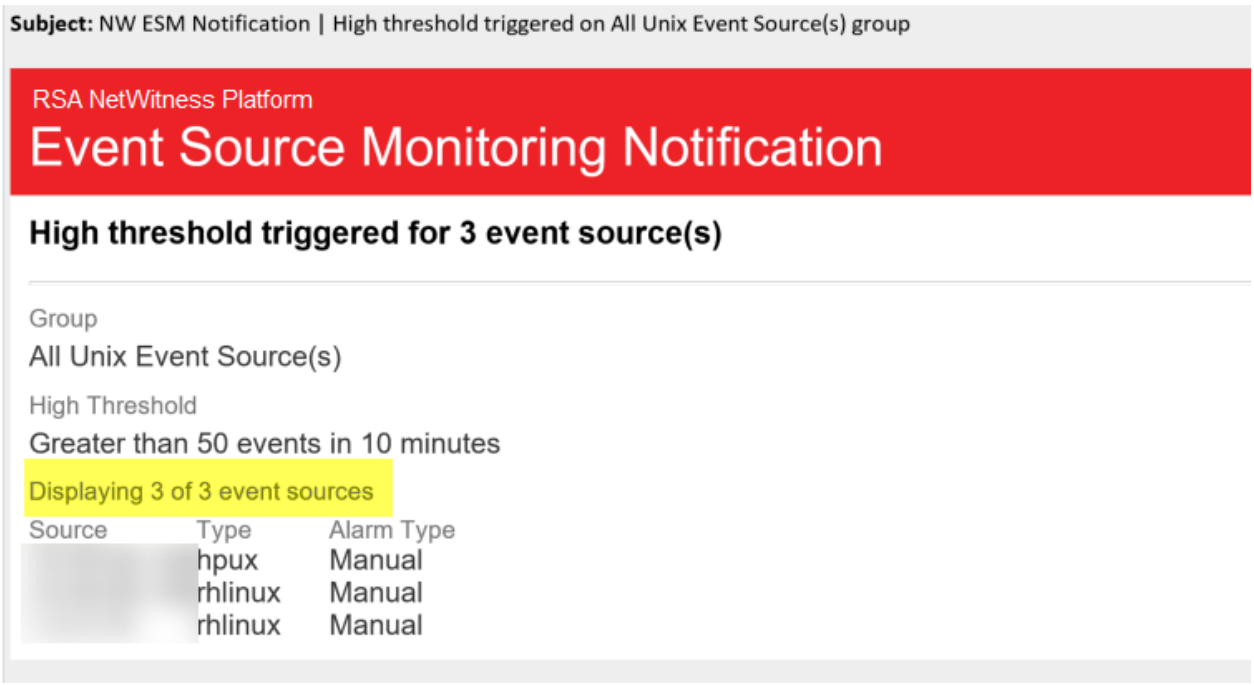
Große E-Mail-Benachrichtigungen

Beachten Sie beim Einrichten von E-Mail-Benachrichtigungen, dass die E-Mail je nach Anzahl der Ereignisquellen in der Benachrichtigung sehr groß werden kann.

Wenn die Anzahl der Ereignisquellen im alarmierten Status 10.000 überschreitet, enthält die E-Mail-Benachrichtigung nur Details zu den ersten 10.000 sowie eine Angabe der Gesamtzahl. Dadurch wird erreicht, dass die E-Mail erfolgreich zugestellt werden kann.

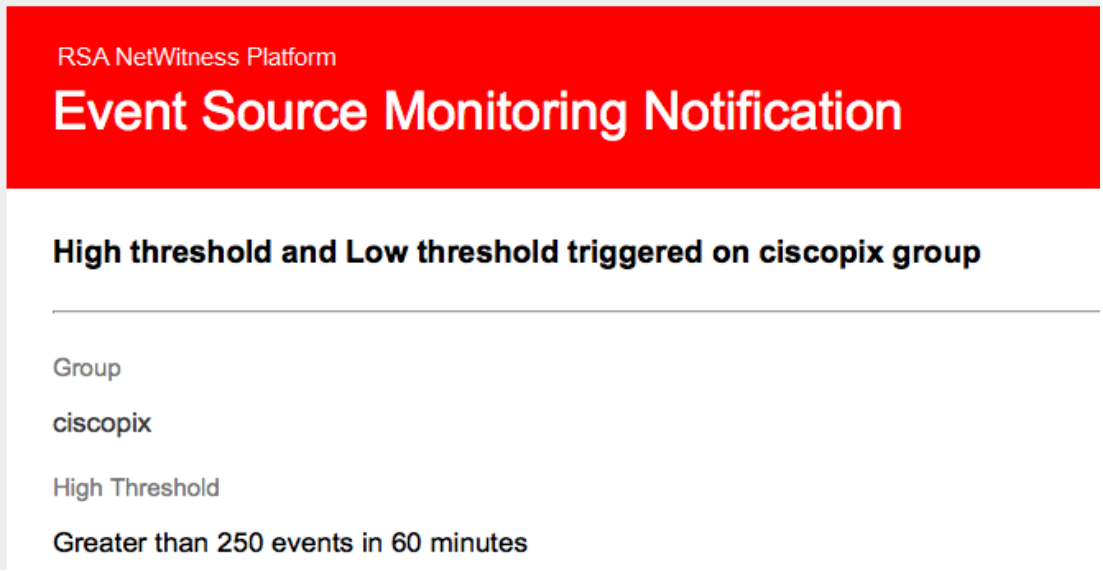
Die folgenden Beispiele zeigen einen für zwei Ereignisquellengruppen ausgelösten unteren Schwellenwert und einen für drei Ereignisquellengruppen ausgelösten oberen Schwellenwert.





Auslösung des oberen und unteren Schwellenwerts

Es kann vorkommen, dass sowohl der obere als auch der untere Schwellenwert einer bestimmten Ereignisquellengruppe ausgelöst werden. Die einfachste Möglichkeit festzustellen, wann dies der Fall ist, ist es, die Kopfzeile der E-Mail zu lesen, in der wie in der folgenden Abbildung zu sehen klar angegeben ist, wenn beide Schwellenwerte ausgelöst werden:



In diesem Beispiel steht in der Kopfzeile „Oberer Schwellenwert und unterer Schwellenwert für Gruppe ciscopix ausgelöst“. Um Details zu den zum unteren Schwellenwert gehörigen Ereignisquellen anzuzeigen, müssen Sie möglicherweise über Hunderte, wenn nicht Tausende zum oberen Schwellenwert gehörige Ereignisquellen hinweg blättern.

Automatische Warnmeldungen

In diesem Thema werden automatische Warnmeldungen beschrieben, die auf Baseline-Einstellungen basieren.

Hinweis: Automatische Warnmeldungen und alle Parameter, die ihr Verhalten bestimmen, sind derzeit im Beta-Test.

Sie können Policies und Schwellenwerte für Ihre Ereignisquellengruppen einrichten. So erhalten Sie Benachrichtigungen, wenn die Schwellenwerte nicht eingehalten werden. NetWitness Platform bietet darüber hinaus eine Methode, Alarme automatisch zu erhalten, wenn Sie keine Schwellenwerte einrichten möchten, um Alarme zu erzeugen.

Um automatische Warnmeldungen auszulösen, können Sie Baselinewerte verwenden. Auf diese Weisemüssen Sie nicht zahlreiche Gruppenschwellenwerte und -Policies einrichten, um Warnmeldungen zu erhalten. Jede ungewöhnliche Menge von Nachrichten löst Warnmeldungen aus, ohne dass eine Konfiguration erforderlich ist (außer dem Einschalten der automatischen Warnmeldungen).

Beachten Sie Folgendes:

- Sobald Sie damit beginnen, Nachrichten aus einer Ereignisquelle zu sammeln, braucht das System etwa eine Woche, um einen Baselinewert für diese Ereignisquelle zu speichern. Nach diesem ersten Zeitraum warnt Sie das System, wenn die Anzahl der Nachrichten für einen Zeitraum um eine bestimmte Menge über oder unter der Baseline liegen. Standardmäßig ist diese Menge 2 Standardabweichungen über oder unter der Baseline.
- Legen Sie Ihre Einstellungen der oberen und unteren Abweichung danach fest, wie „regelmäßig“ Ihre Ereignisquellen sich verhalten. D. h., wenn Sie keine oder nur wenig Abweichung in der Anzahl der

Nachrichten erwarten, die in einem bestimmten Zeitraum eingehen (z. B. 8 bis 9 Uhr an einem Wochentag), können Sie einen niedrigen Wert für die Abweichung festlegen. Wenn Sie andererseits oft sehr hohe Abweichungen sehen, legen Sie den Abweichungswert höher fest.

- Wenn Sie eine Policy aktivieren, aber keine Schwellenwerte festgelegt haben, können Sie dennoch automatische (Baseline-) Benachrichtigungen erhalten, sofern Sie automatische Warnmeldungen aktiviert haben.

Typische Szenarien zu Überwachungsrichtlinien

Typischerweise überwachen viele Unternehmen ihre Ereignisquellen aufgeteilt in Buckets, in Abhängigkeit davon, wie kritisch die einzelnen Ereignisquellen sind. Hier ein typisches Beispiel:

- Angenommen, es existiert eine Gruppe von PCI-Geräten, bei denen es von kritischer Bedeutung ist, innerhalb einer halben Stunde informiert zu werden, wenn eines dieser Gerät das Versenden von Nachrichten einstellt (oder zu wenige Nachrichten sendet).
- Zudem existiert eine andere Gruppe von Windows-Geräten, bei denen es hilfreich ist, innerhalb von vier Stunden informiert zu werden, wenn eines dieser Gerät das Senden von Nachrichten einstellt.
- Und es gibt eine weitere Gruppe mit stillen Geräten, die normalerweise nicht viele Nachrichten senden, bei denen Sie es aber trotzdem erfahren möchten, wenn 24 Stunden lang nichts mehr gesendet wurde.

Viele Unternehmen verfügen möglicherweise über ein Netzwerk, das dem in diesem Beispiel ähnelt. Sie haben möglicherweise weitere oder andere Kategorien, aber in diesem Beispiel wird diese Funktion besprochen.

Auch wenn Sie Dutzende oder gar Hunderte von Ereignisquellengruppen haben sollten, in der Regel gibt es nur wenige Gruppen, für die Sie Schwellenwerte und Warnmeldungen einrichten müssen.

Hinweis: Wenn eine Ereignisquelle Mitglied in mehreren Gruppen ist, für die Warnmeldungen konfiguriert sind, werden die Warnmeldungen nur für die erste übereinstimmende Gruppe in der sortierten Liste ausgegeben. (Die Registerkarte „Überwachungsrichtlinien“ enthält eine sortierte Liste Ihrer Gruppen.)

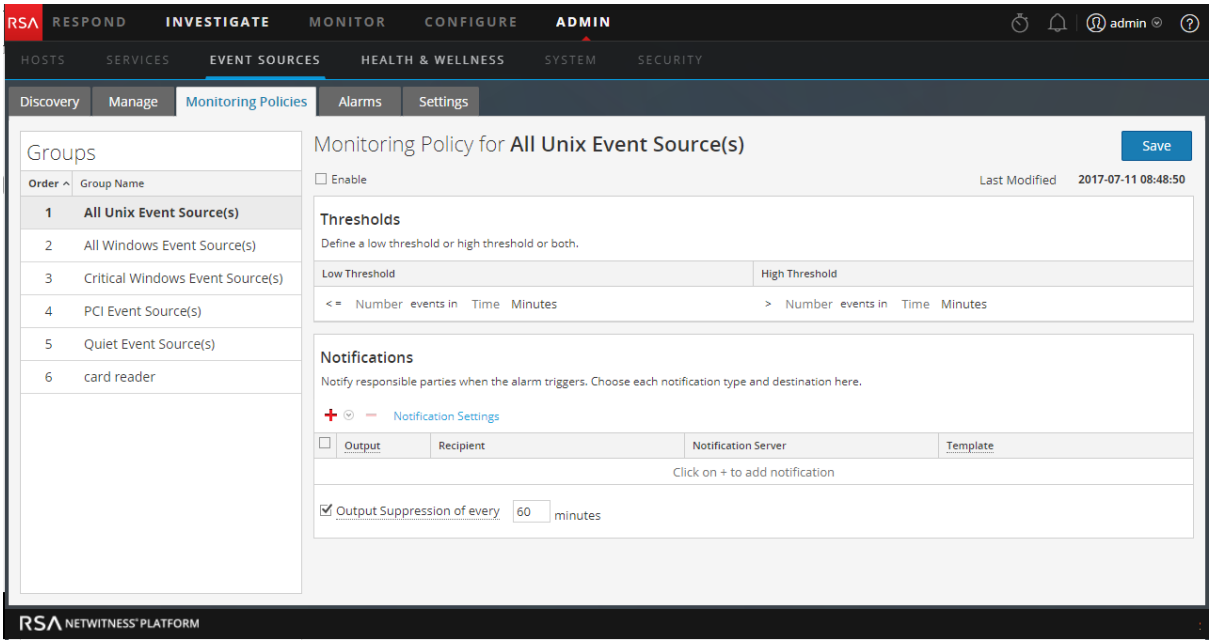
Sortieren der Gruppen

Hinweis: Wenn Sie die Reihenfolge der Gruppen ändern möchten, ziehen Sie eine Gruppe per Drag-and-drop an eine neue Position. Je höher eine Gruppe in der Liste aufgeführt ist, desto höher ist der Rang der Schwellenwerte dieser Gruppe: RSA NetWitness Platform prüft die Schwellenwerte in der Reihenfolge, die in diesem Bereich festgelegt ist. Daher sollten Sie Gruppen mit höchster Priorität ganz oben in der Liste einordnen.

Machen Sie sich klar, in welcher Reihenfolge die Gruppen auf der Seite Überwachungsrichtlinien sortiert werden sollten. Wenn Sie die drei oben erwähnten Gruppen verwenden, sollten Sie diese folgendermaßen anordnen:

1. Stille Ereignisquellen. Indem Sie diese Gruppe an die erste Stelle setzen, können Sie vermeiden, dass Sie übermäßig viele falsche Warnmeldungen erhalten.

2. PCI-Ereignisquellen mit hoher Priorität. Nach den stillen Geräten sollten die Geräte mit der höchsten Priorität folgen.
3. Windows-Ereignisquellen. Für diese Geräte ist der Zeitraum länger als für die PCI-Geräte (vier Stunden gegenüber einer halben Stunde). Daher sollten sie nach den PCI-Geräten angeordnet werden.
4. Alle Ereignisquellen. Optional können Sie Schwellenwerte für alle Geräte definieren, um sämtliche Ereignisse zu erfassen. Auf diese Weise können Sie sicherstellen, dass Ihr gesamtes Netzwerk ordnungsgemäß funktioniert. Für die Catch-All-Gruppe müssen Sie keine Schwellenwerte festlegen. Sie können automatische Warnmeldungen verwenden, um Alarme für die Ereignisquellen in dieser Gruppe zu erzeugen.



Beachten Sie in der obigen Abbildung Folgendes:

- Die Gruppen sind in der oben beschriebenen Reihenfolge angeordnet.
- Der Schwellenwert für PCI-Geräte ist so festgelegt, dass Warnmeldungen versendet werden, wenn die Anzahl der bei NetWitness Platform eingehenden Nachrichten unter 10 Nachrichten in 30 Minuten sinkt.
- Es ist ein unterer Schwellenwert definiert, aber kein oberer. Dies ist in vielen Anwendungsbeispielen der Fall.

Nachdem Sie Ihre Gruppen eingerichtet und sortiert haben und Warnmeldungen erhalten, kann es vorkommen, dass Sie die Reihenfolge nochmals ändern müssen. Beachten Sie beim Ändern der Reihenfolge die folgenden Richtlinien:

- Wenn Sie mehr Benachrichtigungen erhalten als nötig, verschieben Sie die Gruppe in der Reihenfolge nach unten. Analog dazu, wenn Sie zu wenige Benachrichtigungen erhalten, verschieben Sie die Gruppe weiter nach oben.

- Wenn Sie feststellen, dass eine Ereignisquelle mehr Warnmeldungen erzeugt als gewünscht, können Sie diese in eine andere Gruppe verschieben oder eine neue Gruppe für diese Ereignisquelle erstellen.

Managen von Ereignisquellengruppen

Managen von Ereignisquellengruppen

Definitionen

Bedenken Sie bei der Bearbeitung von Ereignisquellengruppen in NetWitness Platform Folgendes:

- Eine **Ereignisquelle** ist im Wesentlichen die Kombination von Werten für alle ihre Attribute.
- Eine **Ereignisquellengruppe** ist der Satz von Ereignisquellen, die einer Reihe von den für diese Gruppe definierten Kriterien entsprechen.

Beispielsweise können folgende Gruppen vorhanden sein:

- Eine Gruppe mit der Bezeichnung **Windows-Geräte**, die alle Ereignisquellentypen umfasst, die Microsoft Windows-Ereignisquellen entsprechen (`winevent_nic`, `winevent_er` und `winevent_snare`).
- Eine Gruppe mit der Bezeichnung **Services mit niedriger Priorität**, die alle Services umfasst, für die das Priority-Attribut auf einen Wert niedriger als 5 festgelegt wurde.
- Eine Gruppe mit der Bezeichnung **Server für Verkäufe in den USA**, in der Sie Ereignisquellen zusammenfassen, die sich in den USA befinden und das Organization-Attribut „Vertrieb“, „Finanzen“ oder „Marketing“ enthalten.

Details zur Registerkarte „Managen“

Die Registerkarte „Managen“ im Modul „Ereignisquelle“ bietet eine einfache Möglichkeit zum Managen von Ereignisquellen. Auf dieser Registerkarte können Sie folgende Aufgaben ausführen:

- Einrichten von Ereignisquellengruppen auf einheitliche Weise
- Arbeiten mit Ereignisquellenattributen auf einheitliche, direkte Weise
- Einfaches Durchsuchen des gesamten Satzes von Ereignisquellen
- Massenbearbeitung und -aktualisierung von Ereignisquellen und Ereignisquellengruppen

Sie können die Details zu Ihren Ereignisquellengruppen anzeigen, indem Sie die folgenden Schritte ausführen:

1. Navigieren Sie zu **ADMINISTRATION** > **Ereignisquellen**.
2. Wählen Sie den Bereich **Managen** aus, um die Details zu Ihren vorhandenen Ereignisquellengruppen einzusehen.

Hinweis: Wenn das System Protokolle von einer Ereignisquelle empfängt, die derzeit nicht in der Ereignisquellenliste vorhanden ist, fügt NetWitness Platform die Ereignisquelle automatisch zur Liste hinzu. Wenn die Ereignisquelle darüber hinaus die Kriterien für eine der vorhandenen Gruppe erfüllt, wird sie Teil dieser Gruppe.

Standardgruppen

RSA NetWitness Platform verfügt über mehrere Standardgruppen. Sie können diese nach Bedarf anpassen und zum Erstellen von neuen Gruppen als Vorlage verwenden.

Folgende Standardgruppen stehen zur Verfügung:

- Alle Ereignisquellen
- Alle Unix-Ereignisquellen
- Alle Windows-Ereignisquellen
- Kritische Windows-Ereignisquellen
- PCI-Ereignisquellen
- In den Ruhemodus versetzte Ereignisquellen

Sie können eine beliebige Gruppen bearbeiten, um die Regeln zu untersuchen, die die Gruppen definieren.

Hinweis: Die Ereignisquellengruppe **Alle** kann nicht bearbeitet oder gelöscht werden.

Erstellen von Ereignisquellengruppen

Administratoren müssen Benachrichtigungen erhalten, wenn Ereignisquellen nicht länger von NetWitness Platform gesammelt werden. Sie müssen in der Lage sein, basierend auf verschiedenen Faktoren zu konfigurieren, wie lange Ereignisquellen still sein können (d. h. keine Protokollnachrichten sammeln), bevor eine Benachrichtigung gesendet wird.

RSA NetWitness Platform stellt Ereignisquellengruppen bereit, damit Sie Geräte mit ähnlicher Wichtigkeit zusammen gruppieren können. Sie können Gruppen basierend auf Attributen erstellen, die Sie aus der CMDB (Konfigurationsmanagement-Datenbank) importiert haben, oder durch manuelles Auswählen von Ereignisquellen, die der Gruppe hinzugefügt werden sollen.

Beispiel: Im Folgenden sind einige der Typen von Ereignisquellengruppen aufgeführt, die Sie erstellen können:

- PCI-Quellen
- Windows Domain Controller
- Stille Quellen
- Finanz-Server
- Geräte mit hoher Priorität
- Alle Windows-Quellen

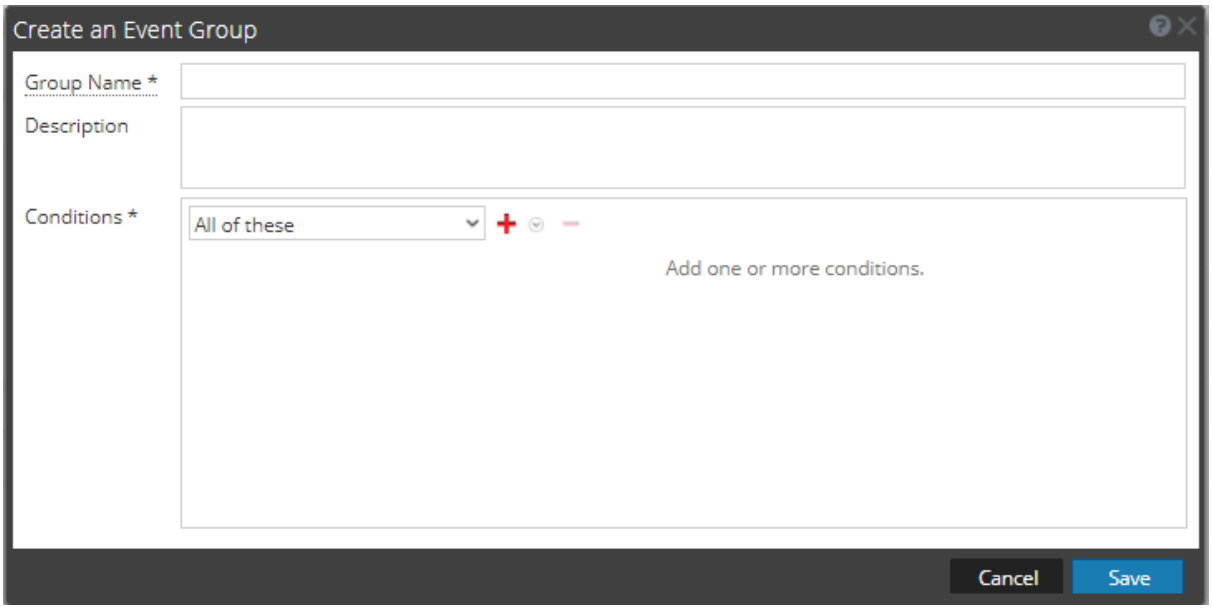
Verfahren

So erstellen Sie eine Ereignisquellengruppe:

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Klicken Sie im Bereich **Verwalten** auf

+.

Das Dialogfeld „Ereignisgruppe erstellen“ wird angezeigt.



3. Geben Sie einen Namen für die Gruppe ein.
4. Geben Sie eine Beschreibung ein
5. Klicken Sie auf +, um eine Bedingung hinzuzufügen. Setzen Sie das Hinzufügen von Bedingungen nach Bedarf fort. Details zum Erstellen von Bedingungen erhalten Sie unter Erstellen/Bearbeiten von Gruppenformularen.
6. Klicken Sie auf **Speichern**.

   Die neue Gruppe wird im Bereich **Verwalten** angezeigt.

Beispiele

In diesem Abschnitt wird ein einfaches Beispiel beschrieben. Anschließend wird erläutert, wie eine komplexerer Regelsatz erstellt wird.

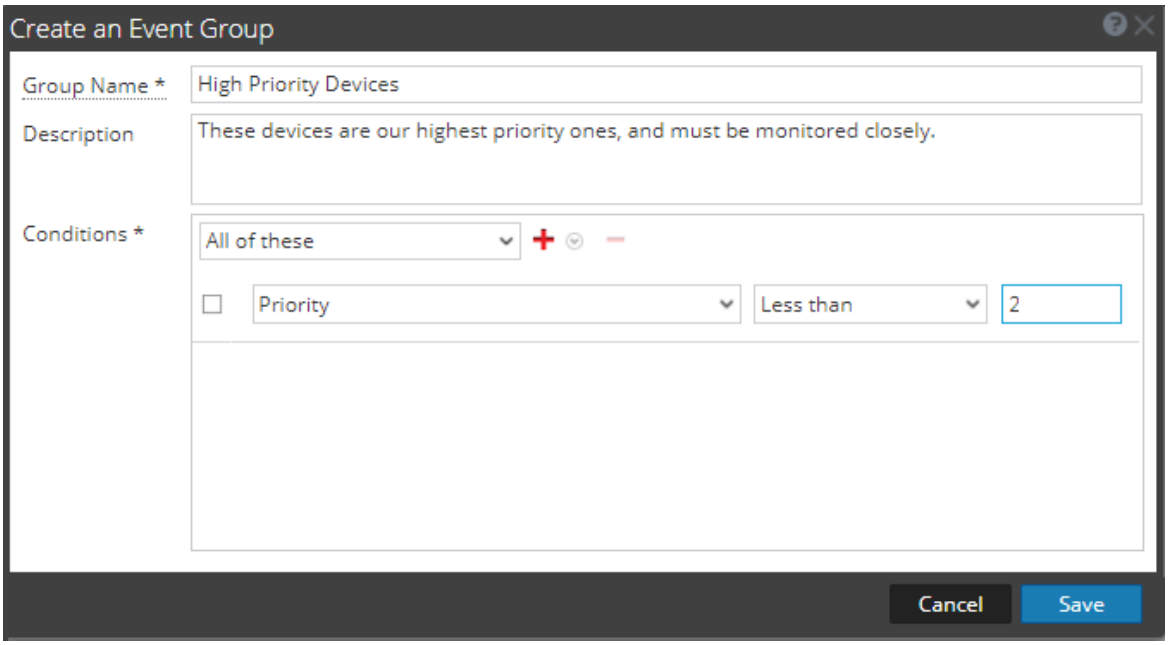
Einfaches Beispiel

In diese Beispiel werde die erforderlichen Schritte beschrieben, wenn Sie eine Ereignisquellengruppe erstellen möchten, die alle Ereignisquellen mit hoher Priorität enthält.

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Klicken Sie im Bereich **Verwalten > Gruppen** auf + .
3. Geben Sie als Gruppenname **Geräte mit hoher Priorität** ein.
4. Geben Sie eine Beschreibung ein, z. B. „Diese Geräte haben die höchste Priorität und müssen engmaschig überwacht werden.“
5. Lassen Sie **Alle diese** ausgewählt und klicken Sie auf + , um eine Bedingung hinzuzufügen.

6. Wählen Sie im Drop-down-Menü **Bedingung hinzufügen** aus.
   a. Wählen Sie ein Attribut aus: **Priorität**.
   b. Wählen Sie einen Operator aus: **Kleiner als**.
   c. Geben Sie einen Wert ein: **2**.

      In der folgenden Abbildung ist das aktualisierte Dialogfeld „Ereignisgruppe bearbeiten“ dargestellt.



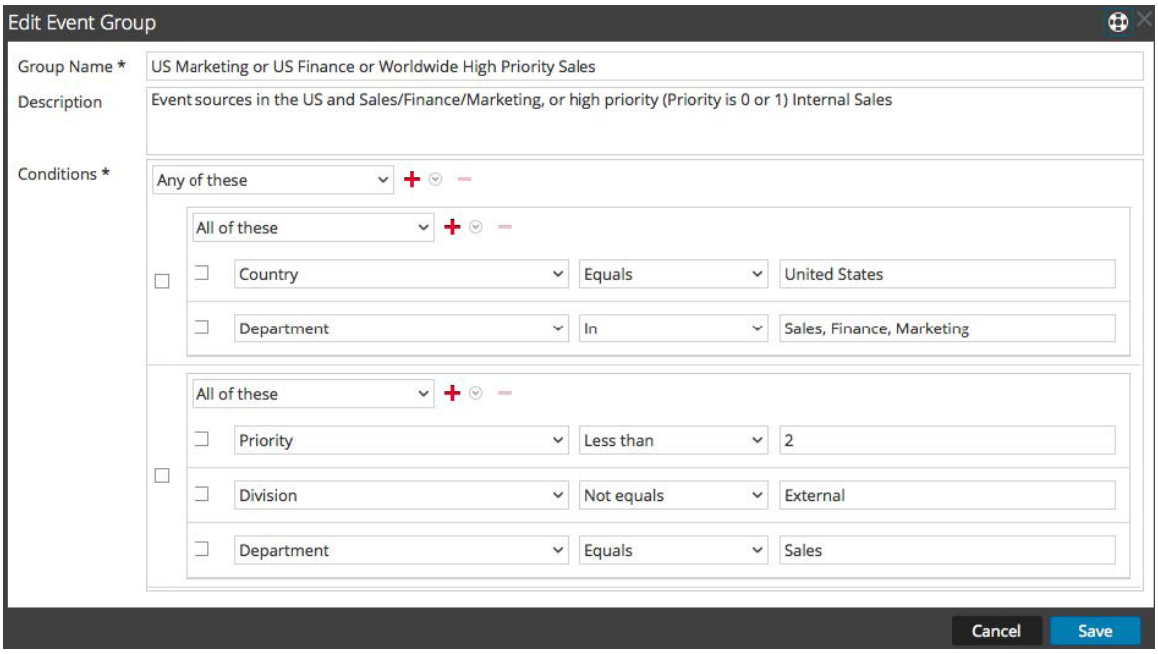
7. Klicken Sie auf **Speichern**.

Komplexes Beispiel

In diesem Beispiel möchten Sie eine relativ komplexe Regel erstellen: Es sollen Ereignisquellen erfasst werden, die sich in den USA befinden und zu den Abteilungen Vertrieb, Finanzen oder Marketing gehören. Außerdem sollen weltweit interne Vertriebsereignisquellen mit hoher Priorität erfasst werden. Als hohe Priorität gilt hierbei eine Priorität von 1 oder 0. Die Definition lautet daher wie folgt:

```
(Country=United States AND (Dept.=Sales OR Dept.=Finance OR
Dept.=Marketing))
 OR
 (Priority < 2 AND Division != External AND Dept.=Sales)
```

Die folgende Abbildung zeigt ein Beispiel für die Kriterien, die Sie beim Erstellen einer solchen Ereignisquellengruppe eingeben würden.



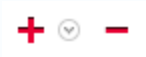
Formular zum Erstellen von Ereignisquellengruppen

Das Formular „Ereignisquellengruppe erstellen“ wird angezeigt, wenn Sie eine Ereignisquellengruppe erstellen oder bearbeiten.

Parameter

In der folgenden Tabelle werden die Felder im Formular zum Erstellen/Bearbeiten einer Ereignisgruppe beschrieben.

Feld	Beschreibung
Gruppenname	Dieses Feld ist erforderlich und wird in der NetWitness Platform-Benutzeroberfläche als Kennung der Gruppe verwendet.
Beschreibung	Eine optionale Beschreibung hilft, den Zweck oder Details zur Gruppe zu umreißen.

Feld	Beschreibung
Tools 	Folgende Optionen sind in der Symbolleiste verfügbar: • **Hinzufügen (+)**: Durch Klicken auf **Hinzufügen** wird ein Menü angezeigt, in dem Sie eine Bedingung oder eine Gruppe hinzufügen können. • **Entfernen (−)**: entfernt die ausgewählte Regel oder Gruppe aus der Liste. Wenn Sie eine neue Gruppe hinzufügen, werden dadurch verschachtelte Bedingungsebene erstellt.
Bedingungen	Eine Beschreibung finden Sie unten in der Tabelle **Regelkriterien**.
Abbrechen/Speichern	Die Optionen **Abbrechen** und **Speichern** sind im Formular verfügbar.

Regelkriterien

Die von Ihnen angegebenen Regeln bestimmen die Ereignisquellen, die in diese Ereignisquellengruppe aufgenommen werden. Eine Regel besteht aus folgenden Elementen:

- Gruppierung: wie die Regel mit anderen Regeln interagiert
- Attribut: welches Attribut die Regel abgleicht
- Operator: wie die Regel das Attribut abgleicht
- Wert: der für die Regel verwendete Attributwert

In der folgenden Tabelle finden Sie Details zu diesen Regelbausteinen.

Regelbaustein	Details
Gruppierung	Sie können Bedingungen gruppieren, um komplexe Regeln für eine Ereignisquellengruppe zu erstellen. Die folgenden Wahlmöglichkeiten haben Sie bei der Gruppierung von Regeln: • **Alle diese**: logisches Äquivalent zu UND • **Beliebige von diesen**: logisches Äquivalent zu ODER • **Nichts davon**: logisches Äquivalent zu NICHT Wenn Sie eine einfache Gruppe erstellen und eine einzige Bedingung angeben, können Sie den Standardwert (**Alle diese**) ausgewählt lassen.
Attribut	Dies enthält eine Drop-down-Liste bestehend aus allen Ereignisquellenattributen. Die Attribute werden nach dem Abschnitt angezeigt, zu dem sie gehören. Beispiel: Zuerst werden alle Attribute zu **Identifikation** angezeigt, gefolgt von den Attributen zu **Eigenschaften**, **Wichtigkeit** usw.

Regelbaustein	Details

Operator	Wählen Sie eine der folgenden Optionen aus:
	• **Gleich**: stimmt mit dem bereitgestellten Wert überein.
	• **Nicht gleich**: gibt Ereignisquellen zurück, deren angegebenes Attribut nicht dem bereitgestellten Wert entspricht.
	• **In**: Sie stellen eine Liste mit Werten im kommagetrennten Format bereit. Ereignisquellen, die einem dieser Werte entsprechen, werden eingeschlossen. Beispiel:
	`Where IP in 10.25.50.146, 10.25.50.248`
	Diese Bedingung gibt Ereignisquellen zurück, die als IP-Attribut `10.25.50.146 or 10.25.50.248` haben.
	• **Nicht in**: ähnlich **In**, es werden aber Elemente ausgegeben, deren Attribut keinem der Listenwerte entspricht.
	• **Wie**: gibt Elemente aus, die mit der angegebenen Zeichenfolge beginnen. Beispiel:
	`Where Event Source Type Like Apache`
	Diese Bedingung gibt Ereignisquellen zurück, deren Ereignisquellentyp mit `Apache` beginnt.
	• **Nicht wie**: ähnlich **Wie**, außer das Elemente zurückgegeben werden, deren Attribut nicht mit der angegebenen Zeichenfolge beginnt.
	• **Größer als**: Gibt Elemente zurück, deren Attribut größer als der angegebene Wert ist. Beispiel: Wenn Sie Priorität größer als 5 angeben, gibt die Bedingung alle Elemente mit einer Priorität von 6 oder höher zurück.
	• **Kleiner als**: ähnlich **Größer als**. Gibt Elemente zurück, deren Attribut kleiner als der angegebene Wert ist.

Wert	Geben Sie einen Wert oder eine Gruppe von Werten an. Der Typ des Werts ist abhängig von dem Attribut für die Bedingung. Beispiel: Bei IPv6 müssen Sie einen Wert im IPv6-Format.

Bestätigen und Zuordnen von Ereignisquellen

In RSA NetWitness® Platform 11.1 hat RSA die automatische Zuordnung eingeführt. Das System ordnet eingehende Ereignisse automatisch anhand früherer Protokolle, die von dieser Adresse erhalten wurden, einem Typ zu und reduziert damit die Anzahl der Elemente, für die Ihre Aufmerksamkeit im Erkennungsworkflow erforderlich ist. Die Benutzeroberfläche gibt an, dass eine Adresse im Erkennungsworkflow automatisch zugeordnet wurde.

Bestätigen von Ereignisquellentypen

Über die Registerkarte „Discovery“ können Sie die Ereignisquellentypen überprüfen, die NetWitness für jede Adresse ermittelt hat, und die Zuverlässigkeit des Systems hinsichtlich der Wahrscheinlichkeit, dass sie korrekt identifiziert wurden. Wenn die erkannten Ereignisquellentypen korrekt sind, können Sie bestätigen, dass diese Ereignisquelle standardmäßig aus der Ansicht herausgefiltert werden soll. Wenn sie falsch sind, können Sie die zulässigen Ereignisquellentypen für eine bestimmte Adresse festlegen, damit zukünftige Protokolle mit dem richtigen Parser analysiert werden.

So bestätigen Sie Ereignisquellen:

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.

   Die Registerkarte „Erkennung“ wird angezeigt.

2. Wählen Sie eine oder mehrere Ereignisquellen aus.
3. Klicken Sie auf **Bestätigung umschalten**.

Beachten Sie Folgendes:

- Sobald die Ereignisquellen bestätigt wurden, werden sie nicht mehr in der Spalte „Ereignisquelltyp (en)“ angezeigt.
- Die Schaltfläche **Bestätigung umschalten** verhält sich folgendermaßen:
  - Wenn der bestätigte Zustand für alle ausgewählten Ereignisquellen identisch ist, werden alle Werte umgeschaltet. Das heißt, wenn Sie nur Ereignisquellen mit **Ja** in der Spalte „Bestätigt“ auswählen, wird der Wert für alle in **Nein** geändert. Entsprechend wird der Wert für alle ausgewählten Ereignisquellen in **Ja** geändert, wenn für alle der Wert **Nein** ausgewählt ist.
  - Wenn Sie mehrere Ereignisquellen auswählen und für einige der Wert **Ja** und für andere der Wert **Nein** ausgewählt ist, werden durch Klicken auf **Bestätigung umschalten** alle Werte für die ausgewählten Ereignisquellen auf **Ja** festgelegt.

Hinweis: Bestätigte Ereignisquellen werden standardmäßig nicht angezeigt.

Manuelles Zuordnen von Kartenereignissen

Wenn die erkannten Ereignisquellentypen nicht vollständig korrekt sind, können Sie die Parser zuordnen, um zusätzliche Informationen zu erhalten.

So ordnen Sie eine oder mehrere Ereignisquellen zu:

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.

   Die Registerkarte „Erkennung“ wird angezeigt.

2. Wählen Sie eine oder mehrere Ereignisquellen aus.

3. Klicken Sie auf Map .

   Das Dialogfeld „Parser-Zuordnungen verwalten“ wird angezeigt.

4. Fügen Sie Parser-Zuordnungen hinzu oder entfernen Sie sie und ändern Sie die Prioritätsreihenfolge basierend auf den Bedürfnissen Ihrer Organisation. Nähere Informationen finden Sie unter Parser-Zuordnungen verwalten .

Hinweis: Discovery Scores für die zugeordneten Ereignisquellen werden in der Spalte „Ereignisquelltyp(en)“ vom niedrigsten zum höchsten Discovery Score aufgeführt. Discovery Scores reichen von 0 (geringstes Vertrauen) bis 100 (stärkstes Vertrauen).

Anzeigen von Protokollen von einer Log Decoder-Version vor 11.0

In RSA NetWitness® Platform 11.0 besteht nun die Möglichkeit, eine kleine Auswahl der letzten Protokolle für bestimmte Geräte auf den jeweiligen Detail-Registerkarten der Ansicht „Erkennung“ anzuzeigen. Standardmäßig besitzen Log Decoder vor Version 11.0 nicht die erforderliche Konfiguration zum Aktivieren dieser Funktion. Dies ist jedoch durch Vornehmen einiger geringfügiger Änderungen möglich. Weitere Informationen finden Sie unter Anzeigen von Protokollen von einer Log Decoder-Version vor 11.0.

Bearbeiten oder Löschen von Ereignisquellengruppen

Es kann gelegentlich vorkommen, dass Sie eine Ereignisquellengruppe löschen müssen. Wenn Sie zum Beispiel ein Büro schließen und über eine Gruppe verfügten, die aus allen Ereignisquellen in diesem Büro bestand, können Sie die Gruppe löschen, da keine dieser Ereignisquellen mehr Informationen an NetWitness Platform sendet.

Oder vielleicht müssen Sie einige der Bedingungen ändern, unter denen die Gruppe befüllt wird.

Hinweis: Sie können den Namen der Ereignisquellengruppe nicht bearbeiten. Nachdem Sie eine Gruppe erstellt haben, besteht der Name so lange, wie die Gruppe selbst besteht.

Bearbeiten einer Ereignisquellengruppe

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie im Bereich **Managen** eine vorhandene Ereignisquellengruppe aus.
3. Klicken Sie auf .

   Das Dialogfeld Ereignisgruppe bearbeiten wird angezeigt.

4. Ändern Sie Details oder fügen Sie Bedingungen hinzu, bearbeiten oder löschen Sie sie nach Bedarf.
5. Klicken Sie auf **Speichern**.

Löschen einer Ereignisquellengruppe

Beachten Sie Folgendes:

- Sie können jede beliebige Gruppe löschen, mit Ausnahme der Gruppe **Alle**, die alle konfigurierten Ereignisquellen im System auflistet.
- Wenn Sie eine Gruppe löschen, wird auch die zugehörige Policy für diese Gruppe automatisch gelöscht.
- Wenn Ereignisquellen **nur** zu der gelöschten Gruppe gehören, wäre ihnen kein Policy-Alarm mehr zugeordnet. Denken Sie daran, dass Ereignisquellen zu mehreren Gruppen gehören können.
- Das Löschen einer Gruppe hat keine Auswirkung auf die Baseline-Alarme.

So löschen Sie eine Ereignisquellengruppe:

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Wählen Sie im Bereich **Managen** eine vorhandene Ereignisquellengruppe aus.
3. Klicken Sie auf .
   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Ja**, um die Gruppe zu löschen.

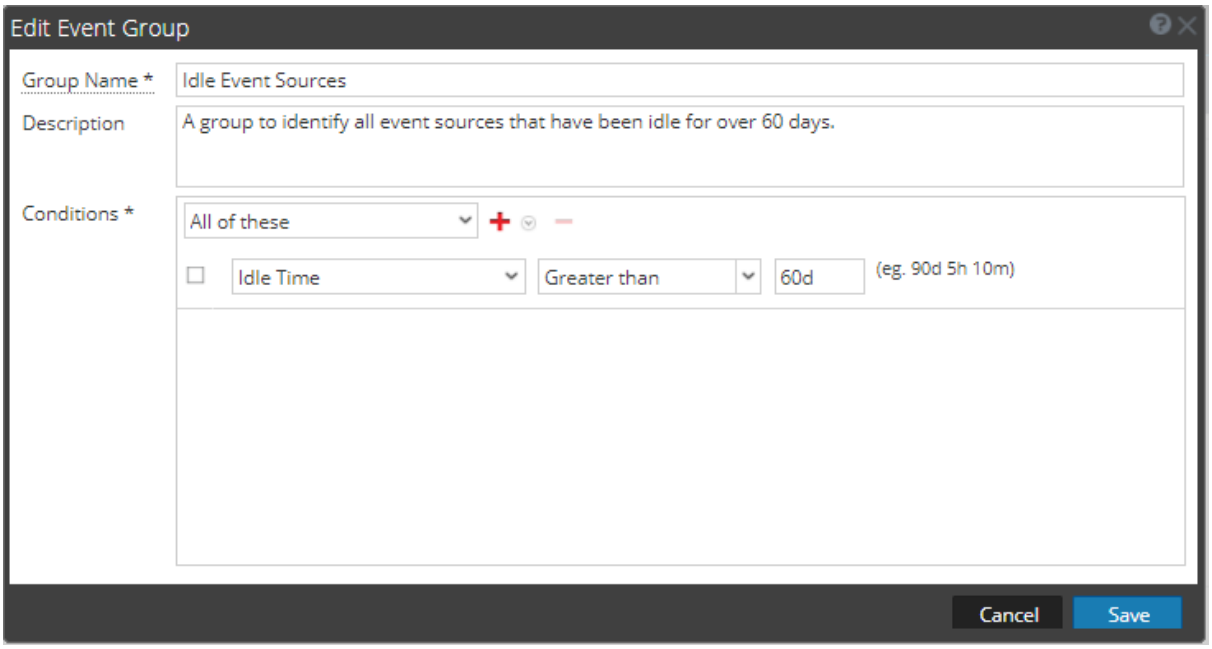
Entfernen inaktiver Ereignisquellen

Sie können Ihre Gruppe von Ereignisquellen in regelmäßigen Abständen aktualisieren und diejenigen entfernen, die nicht mehr verwendet werden. Dazu können Sie den Parameter **Inaktivitätsdauer** verwenden.

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.2 und höher.

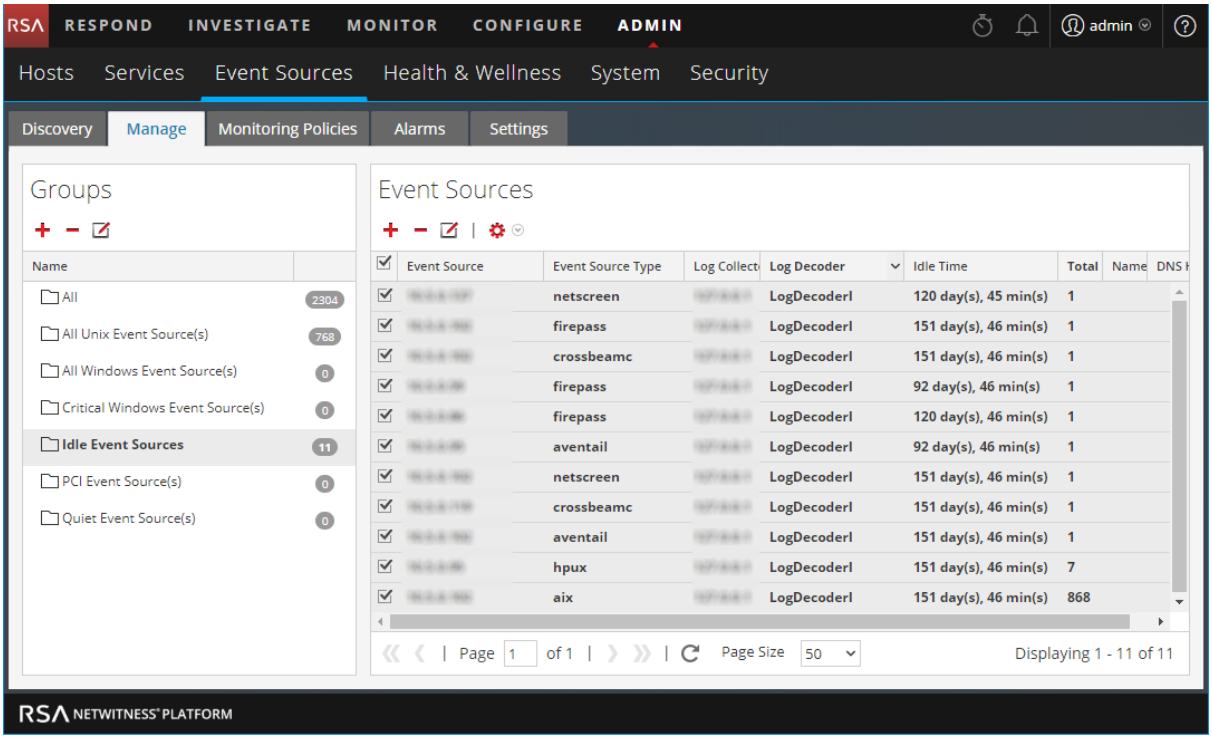
So entfernen Sie inaktive Ereignisquellen:

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Klicken Sie im Bereich **Verwalten** auf  .
   Das Dialogfeld „Ereignisgruppe erstellen“ wird angezeigt.
3. Geben Sie den Namen und die Beschreibung wie gewünscht ein, und fügen Sie eine Bedingung hinzu, die den Parameter **Inaktivitätsdauer** verwendet, wie nachfolgend gezeigt:



In diesem Beispiel wurde die Bedingung so festgelegt, dass Ereignisquellen identifiziert werden, die seit mindestens 60 Tagen inaktiv sind.

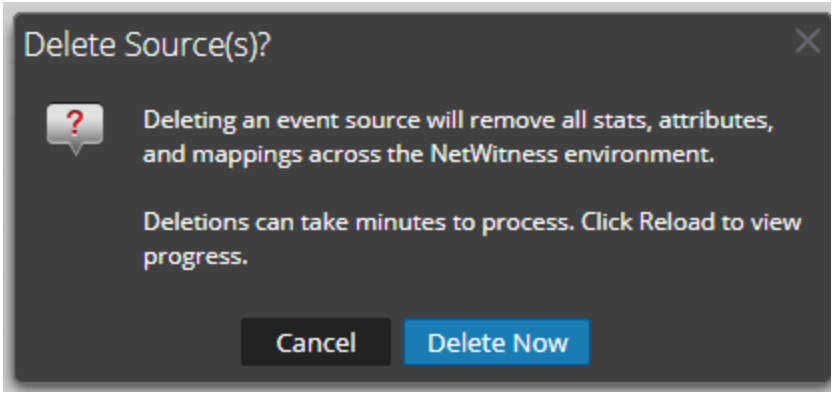
4. Speichern Sie die neue Gruppe und wählen Sie sie dann im Bereich „Gruppen“ aus.
5. Wählen Sie einige oder alle Ereignisquellen in der Gruppe aus. Der folgende Bildschirm zeigt alle aus dieser Gruppe ausgewählten Ereignisquellen an.



6. Klicken Sie im Bereich „Ereignisquellen“ auf

, um die ausgewählten inaktiven Ereignisquellen zu löschen.

Es wird eine Bestätigungsmeldung angezeigt:



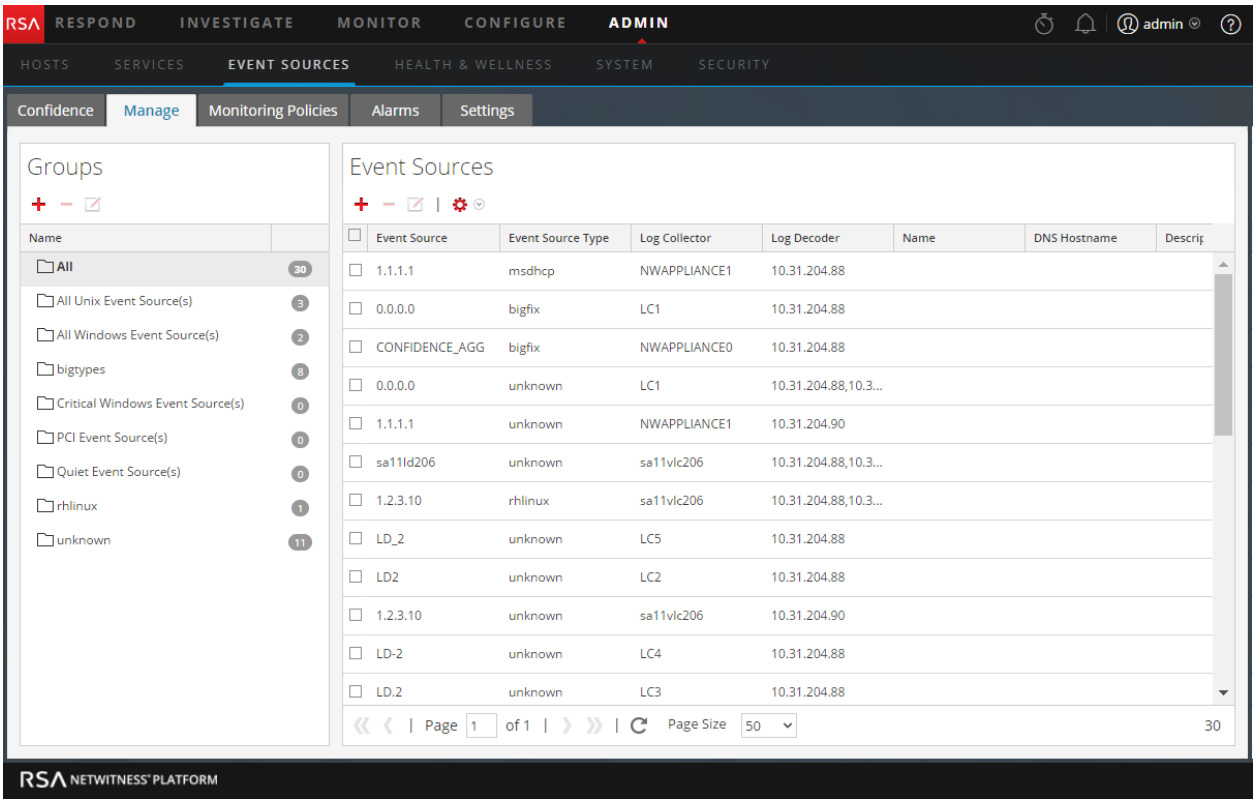
7. Klicken Sie auf „Jetzt löschen“, um das Löschen der ausgewählten Ereignisquellen zu bestätigen.

Wenn in Zukunft eine entfernte Ereignisquelle Protokolle sendet, wird eine neue Ereignisquelle erstellt.

Erstellen von Ereignisquellen und Bearbeiten von Attributen

Sie können Ereignisquellen in Gruppen organisieren. Dazu geben Sie Werte für verschiedene Attribute jeder Ereignisquelle ein. Beispiel: Sie können für alle Ereignisquellen mit hoher Priorität den Wert für **Priorität** auf 1 festlegen. Einzelheiten zu den verfügbaren Attributen erhalten Sie im Thema Registerkarte „Ereignisquelle verwalten“.

Die folgende Abbildung zeigt ein Beispiel für den Bereich Ereignisquellen:



Ereignisquellenattribute bestehen aus einer Kombination von automatisch ausgefüllten und vom Benutzer eingegebenen Informationen. Wenn eine Ereignisquelle Protokollinformationen an NetWitness Platform sendet, wird sie der Liste der Ereignisquellen hinzugefügt und einige grundlegende Informationen werden automatisch ausgefüllt. Danach kann der Benutzer jederzeit Details zu anderen Ereignisquellenattributen hinzufügen oder bearbeiten.

Obligatorische Attribute

Die folgenden Identifizierungsattribute werden besonders behandelt: **IP**, **IPv6**, **Hostname**, **Ereignisquelltyp**, **Log Collector** und **Log Decoder**. Wenn Sie eine Ereignisquelle manuell erstellen, können Sie diese Werte eingeben. Sobald Sie die Ereignisquelle speichern, können diese Werte nicht mehr geändert werden.

Ereignisquellen können auch automatisch erkannt werden. Jede Ereignisquelle, die Meldungen an den Log Decoder sendet, wird der Liste der Ereignisquellen hinzugefügt. Beim Bearbeiten der Attribute einer automatisch erkannten Ereignisquelle können Sie keines dieser Felder bearbeiten.

Beachten Sie, dass nicht alle diese Felder obligatorisch sind. Zur eindeutigen Identifikation einer Ereignisquelle sind folgende Informationen erforderlich:

- IP, IPv6 oder Hostname und
- Ereignisquellentyp

Außerdem verwendet RSA NetWitness Platform eine Hierarchie für IP, IPv6 und Hostname. Die Reihenfolge lautet wie folgt:

1. IP
2. IPv6

3. Hostname

Beim manuellen Eingeben von Ereignisquellen müssen Sie diese Reihenfolge beachten. Andernfalls kann es beim Empfangen von Meldungen von den manuell konfigurierten Ereignisquellen zu Duplikaten kommen.

Alle anderen Attribute (z. B. Priorität, Land, Unternehmen, Anbieter usw.) sind optional.

Erstellen von Ereignisquellen

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Managen** aus.
3. Klicken Sie im Bereich **Ereignisquellen** auf + , um den Detailbildschirm zu öffnen, der alle Ereignisquellenattribute enthält.

   Die Registerkarte „Ereignisquelle verwalten“ wird angezeigt.
4. Geben Sie Werte für Attribute ein oder ändern Sie diese.
5. Klicken Sie auf **Speichern**.

Hinweis: Der Discovery Score ist für manuell hinzugefügte Ereignisquellen als **Nicht verfügbar** aufgeführt. Der Score bleibt als **Nicht verfügbar** gekennzeichnet, bis die Ereignisquelle beginnt, Informationen an RSA NetWitness® Platform zu senden.

Aktualisieren von Attributen einer Ereignisquelle

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Managen** aus.
3. Wählen Sie im Bereich **Ereignisquellen** eine Ereignisquelle in der Liste aus.
4. Klicken Sie im Bereich **Ereignisquellen** auf + , um den Detailbildschirm zu öffnen, der alle Ereignisquellenattribute enthält.

   Die Registerkarte „Ereignisquelle verwalten“ wird angezeigt.
5. Geben Sie die Werte für Attribute ein oder ändern Sie diese. Einige Attributwerte können jedoch nicht verändert werden, nachdem sie einmal eingegeben wurde.
6. Klicken Sie auf **Save**

Massenbearbeitung von Ereignisquellenattributen

Sie können mehrere Ereignisquellen, eine komplette Gruppe oder gar alle Ereignisquellen zur Massenbearbeitung auswählen. Beispielsweise können Sie die Priorität oder den Manager für eine große Anzahl von Ereignisquellen gleichzeitig ändern.

Hinweis: Sie können jedoch nicht einzelne Ereignisquellen auf mehreren angezeigten Seiten auswählen. Wenn Sie beispielsweise eine Gruppe mit 225 Ereignisquellen haben und die Seitengröße 50 festgelegt haben, können Sie nur Ereignisquellen aus den angezeigten 50 Elementen auswählen.

Zum Bearbeiten von Elementen, die sich auf mehreren Seiten befinden, gibt es folgende Möglichkeiten:

- Erhöhen Sie im Browser die Seitengröße (das Maximum sind 500 Einträge pro Seite). Falls Sie eine kleine Seitengröße gewählt haben, können Sie vielleicht alle Elemente auf einer einzelnen Seite unterbringen.
- Erstellen Sie eine neue Ereignisquellengruppe, die nur die Elemente enthält, die Sie per Massenbearbeitung ändern möchten. Anschließend können Sie alle Elemente dieser Gruppe statt einzelner Elemente der Gesamtmenge auswählen.
- Führen Sie die Massenbearbeitung in mehreren Schritten aus. Wählen Sie auf der ersten Seite die Elemente aus, die Sie bearbeiten möchten. Nehmen Sie die Änderungen vor. Gehen Sie dann zu nächsten Seite und wiederholen Sie den Vorgang, bis alle gewünschten Änderungen durchgeführt sind.

Hinweis: Obligatorische Felder können nicht bearbeitet werden: IP, IPv6, Hostname, Ereignisquelltyp, Log Collector und Log Decoder.

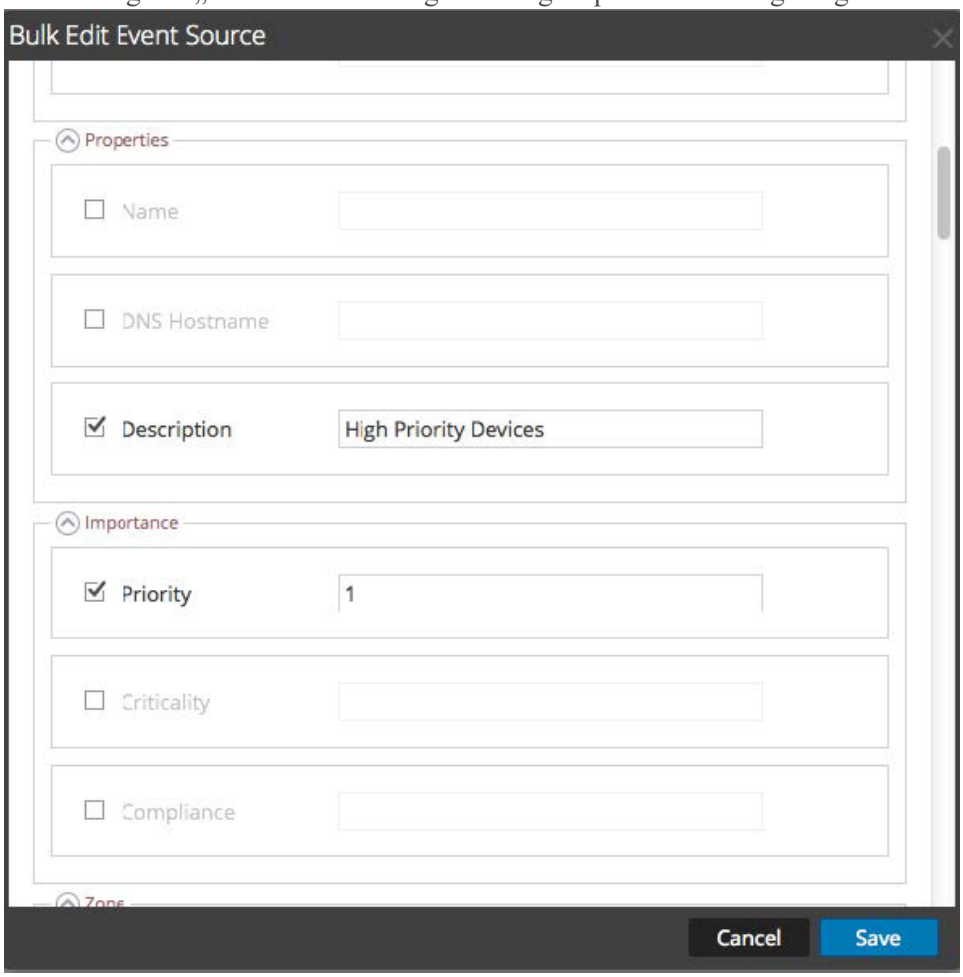
So ändern Sie Attribute für Ereignisquellen per Massenbearbeitung:

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Managen** aus.
3. Optional: Wählen Sie eine Ereignisquellengruppe aus.
4. Wählen Sie im Bereich **Ereignisquellen** eine oder mehrere Ereignisquellen aus, die bearbeitet werden sollen.

   Hinweis: Um alle Ereignisquellen auszuwählen, aktivieren Sie das Kontrollkästchen neben der Spalte **Aktionen** in der letzten Spalte der Listentabelle (ganz rechts).

5. Klicken Sie in der Menüleiste auf das Symbol **Bearbeiten** .

Das Dialogfeld „Massenbearbeitung für Ereignisquelle“ wird angezeigt.



6. Geben Sie Werte für jedes der verfügbaren Attribute ein. Im oben abgebildeten Screenshot wurden die Attribute Name und Priorität aktualisiert.
7. Nachdem Sie die erforderlichen Attribute aktualisiert haben, klicken Sie auf **Speichern**.

Importieren von Ereignisquellen

Sie können Ereignisquellenattribute aus einer CSV-formatierten Datei importieren. Um Informationen aus einer CMDB (Configuration Management Database), einer Tabelle oder einer anderen Datei zu importieren, müssen Sie die Informationen zunächst in eine CSV-Datei konvertieren oder als solche speichern.

Hinweis: Die folgenden Identifizierungsattribute werden besonders behandelt: **IP**, **IPv6**, **Hostname**, **Ereignisquelltyp**, **Log Collector** und **Log Decoder**. Wenn Sie eine Ereignisquelle importieren, die für eines dieser Felder einen anderen Wert enthält (verglichen mit dem Wert in NetWitness Platform), wird der ursprüngliche Wert in NetWitness Platform **nicht** überschrieben.

Die importierten Attribute werden der zugehörigen Ereignisquelle zugewiesen und stehen zur Verwendung in Regeln für die Erstellung von Ereignisquellengruppen zur Verfügung.

RSA NetWitness Platform behandelt die Importdatei als den korrekten, vollständigen Datensatz. Daraus resultieren die folgenden Verhaltensweisen im Zusammenhang mit dem Importieren von Ereignisquellenattributen:

- Standardmäßig werden beim Importieren von Attributen nur Attribute vorhandener Ereignisquellen durch das System aktualisiert.
- Wenn die Ereignisquelle zwar in der Importdatei, nicht aber in NetWitness Platform vorhanden ist, werden die Attribute für diese Ereignisquelle ignoriert. Das bedeutet, NetWitness Platform erstellt **keine** neuen Ereignisquellen für diese Attribute.
- Wenn die Ereignisquelle in der Importdatei und in NetWitness Platform vorhanden ist, werden die Werte für diese Ereignisquelle überschrieben.
- Wenn ein Attribut in der Importdatei leer ist, wird das entsprechende Attribut in NetWitness Platform entfernt.
- Wenn ein Attribut in der Importdatei nicht spezifiziert ist, wird das entsprechende Attribut in NetWitness Platform ignoriert (d. h., der Wert wird **nicht** entfernt).

Hinweis: Es gibt einen Unterschied zwischen einem leeren Attribut und einem nicht spezifizierten Attribut. Wenn ein Attribut angegeben aber leer ist, wird vorausgesetzt, dass es leer sein soll, und NetWitness Platform entfernt den Wert für das Attribut für die zugehörige Ereignisquelle. Wenn ein Attribut jedoch überhaupt nicht spezifiziert ist, wird vorausgesetzt, dass keine Änderung erwartet wird.

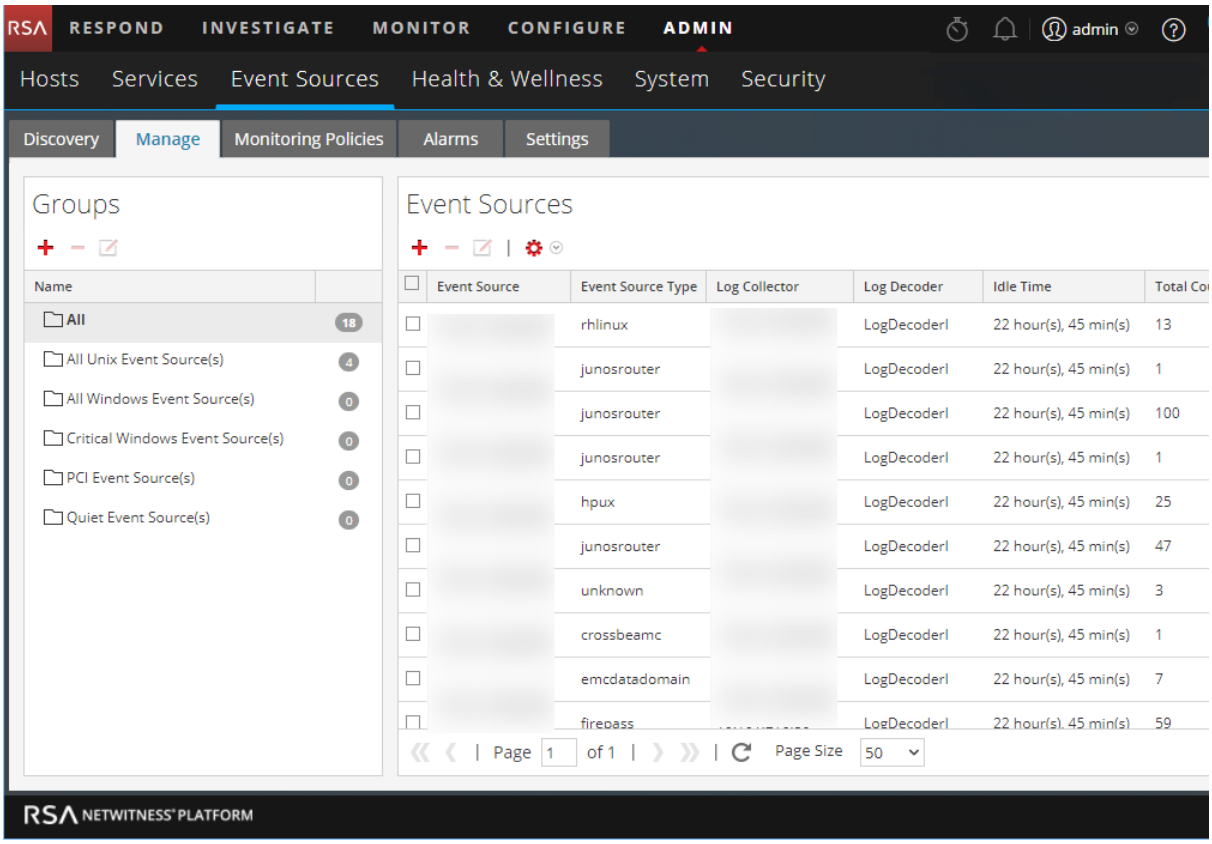
Die obigen Verhaltensweisen sind Standardverhalten – Sie können diese wie im folgenden Verfahren angegeben ändern.

Importieren von Ereignisquellenattributen

So importieren Sie Ereignisquellenattribute aus einer Datei:

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Verwalten** aus.

   Die Ansicht „Ereignisquellen“ wird auf der Registerkarte „Verwalten“ angezeigt.



3. Wählen Sie im Menü „Importieren/Exportieren“ in der Symbolleiste ( ) die Option **Importieren** (Import) aus.

   Das Dialogfeld Ereignisquelle hinzufügen wird angezeigt.

4. Navigieren Sie zu der Importdatei und aktivieren Sie die entsprechenden Kästchen:

- **Standard**: Das Standardverhalten ist oben beschrieben.
- **Nur hinzufügen**: Importiert ein Attribut nur, wenn das entsprechende Feld in NetWitness Platform leer ist. Es werden also keine vorhandenen Werte überschrieben.
- **Werte nicht löschen**: Die Attributwerte in NetWitness Platform für Elemente, die in der Importdatei leer sind, werden nicht gelöscht.
- **Unbekannte Quellen hinzufügen**: Fügt basierend auf den Elementen in der Importdatei neue Ereignisquellen hinzu.

Hinweis: Sie können mehrere Optionen auswählen.

5. Klicken Sie auf **Import**.
6. Klicken Sie auf **Ja** im Bestätigungsdialogfeld, um den Import durchzuführen.

Troubleshooting der Importdatei

Wenn die Importdatei nicht korrekt formatiert ist oder erforderliche Informationen fehlen, wird ein Fehler angezeigt und die Datei wird nicht importiert.

Überprüfen Sie Folgendes:

- Wenn Sie unbekannte Quellen hinzufügen, muss jede Zeile in der Datei eine Kombination der erforderlichen Attribute enthalten:
  - IP, IPv6 oder Hostname und
  - Ereignisquelltyp
- Die erste Zeile der Datei muss Header-Namen enthalten, die mit den Namen in NetWitness Platform übereinstimmen. Sie können eine einzelne Ereignisquelle exportieren, um eine Liste der korrekten Header-Namen zu erhalten. Betrachten Sie die exportierte CSV-Datei: die erste Zeile der Datei enthält den korrekten Satz Attribute/Spaltennamen.

Wenn die Importdatei nicht korrekt formatiert ist oder erforderliche Informationen fehlen, wird ein Fehler angezeigt und die Datei wird nicht importiert.

Exportieren von Ereignisquellen

Sie können alle oder einige Ereignisquellen zusammen mit den entsprechenden Attributen in eine CSV-Datei exportieren.

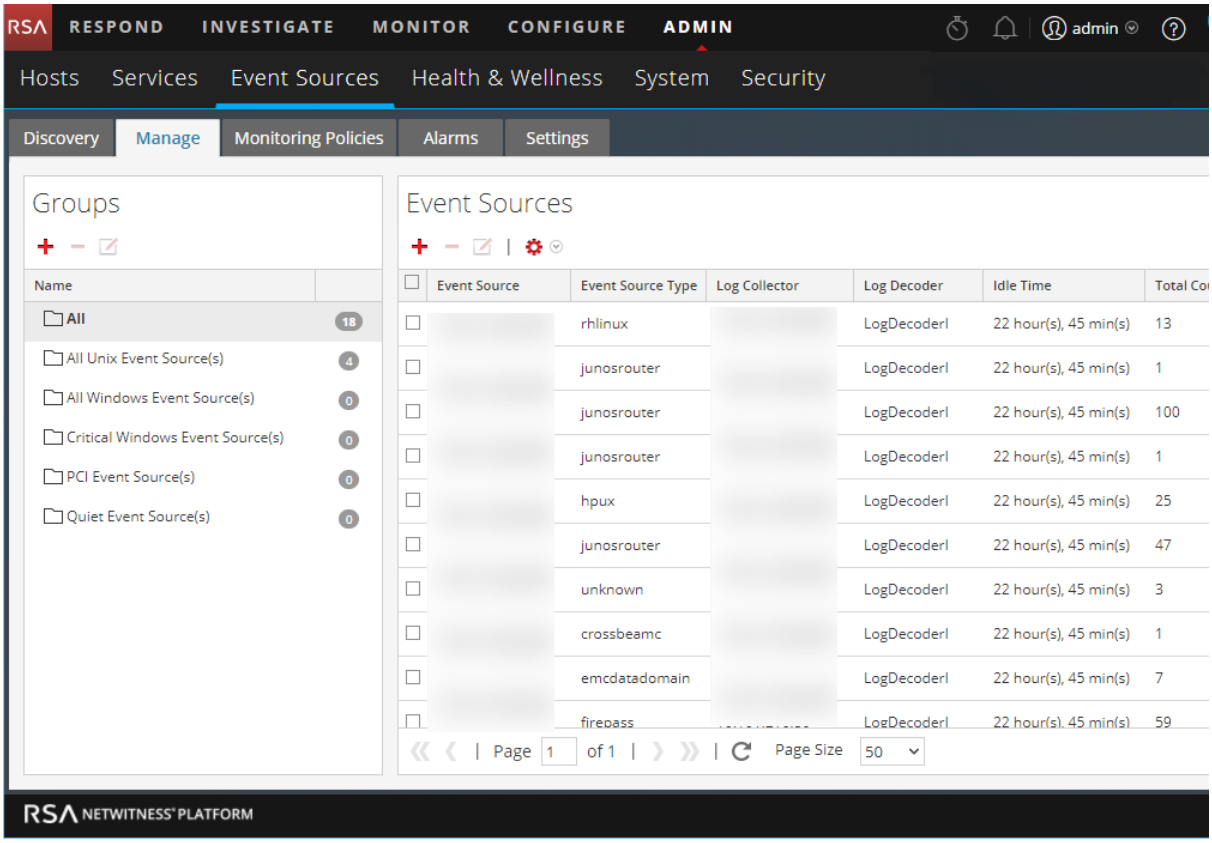
Beachten Sie Folgendes:

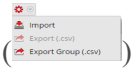
- Die exportierte CSV-Datei enthält alle Attributspalten.
- Die exportierte CSV-Datei enthält eine Kopfzeile, in der die Spaltennamen aufgeführt sind.
- Sie können alle Einträge in eine Gruppe exportieren.
- Sie können alle Einträge exportieren (wählen Sie die Gruppe **Alle** aus.
- Sie können Einträge auswählen und nur diese Einträge exportieren.

So exportieren Sie Ereignisquellen:

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Verwalten** aus.

   Die Ansicht „Ereignisquellen“ wird auf der Registerkarte „Verwalten“ angezeigt.



3. Wählen Sie die Gruppe aus, die die zu exportierenden Ereignisquellen enthält.
4. Wählen Sie so viele Ereignisquellen aus, wie Sie benötigen. Alternativ können Sie die gesamte Gruppe exportieren. Dazu müssen Sie keine einzelnen Ereignisquellen auswählen.
5. Wählen Sie im Menü „Importieren/Exportieren“ in der Symbolleiste () die Option **Exportieren (.csv)** oder **Gruppe exportieren (.csv)** aus.

   Das Dialogfeld „Ereignisquellen exportieren“ wird angezeigt.

6. Geben Sie einen Dateinamen ein und klicken Sie auf **Exportieren**.

Die Ereignisquellenattribute werden im CSV-Format unter dem von Ihnen angegebenen Dateinamen gespeichert.

Sortieren von Ereignisquellen

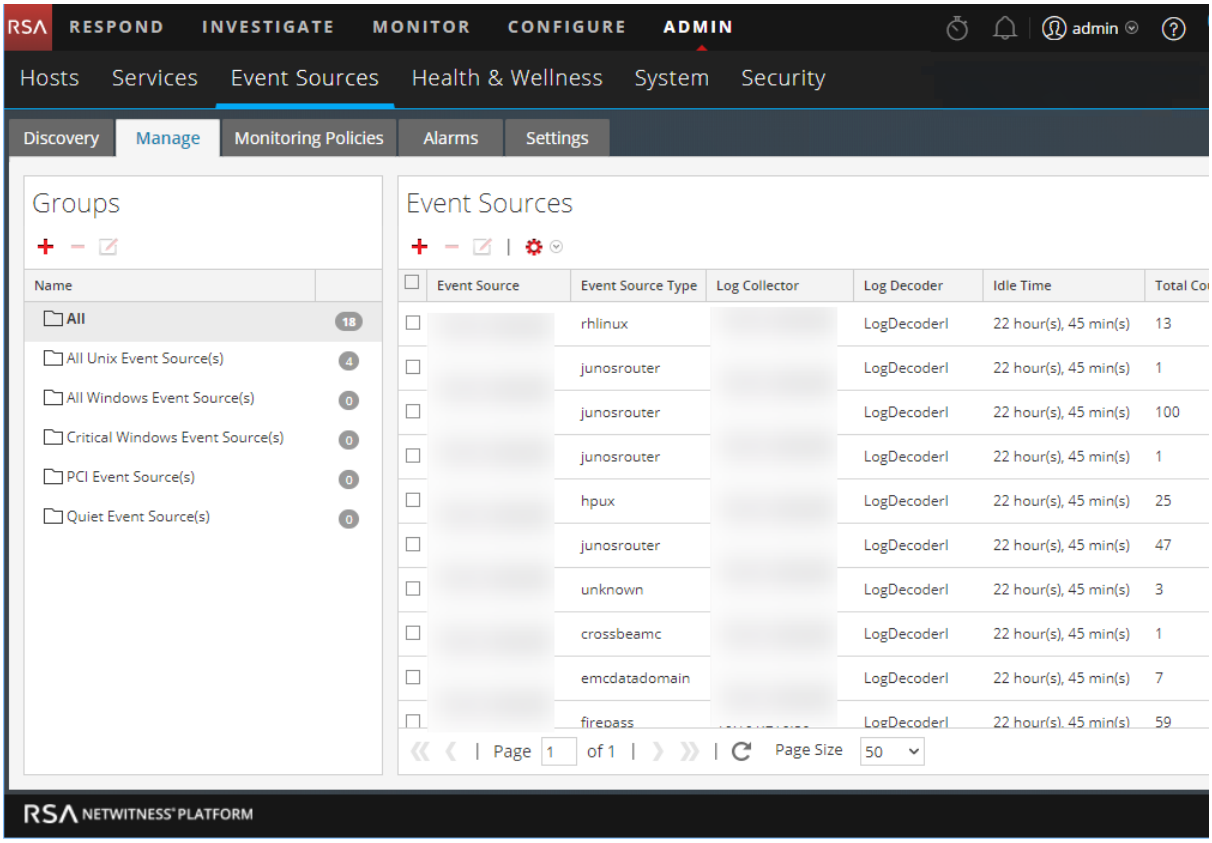
Im Ereignisquellenbereich werden Attribute für die aktuell ausgewählte Ereignisquellengruppe angezeigt. Sie können die Liste der angezeigten Attribute konfigurieren sowie die Liste anhand eines der angezeigten Attribute sortieren.

Hinweis: Es wird gesamte Liste sortiert, nicht nur die auf der aktuellen Seite angezeigten Elemente. (Die Navigationsleiste unten auf der Seite zeigt an, wie viele Seiten die Liste der Ereignisquellen hat.)

So sortieren Sie Ereignisquellen:

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Verwalten** aus.

   Die Ansicht „Ereignisquellen“ wird auf der Registerkarte „Verwalten“ angezeigt.



3. Klicken Sie zum Sortieren einer Spalte in der Kopfzeile der Spalte auf +.

   Das Drop-down-Menü Sortieroptionen wird angezeigt.
4. Wählen Sie die gewünschte Sortierreihenfolge aus.

Richtlinien managen

Überwachungsrichtlinien

Über die Ansicht Überwachungsrichtlinien können Sie die Warnmeldungskonfiguration für die Ereignisquellengruppen managen.

Durch Festlegen von Schwellenwerten und Benachrichtigungen erstellen Sie Warnmeldungsrichtlinien für Ereignisquellengruppen:

- Mit Schwellenwerten legen Sie die Bereiche für die Häufigkeit von Protokollmeldungen fest. Geben Sie einen unteren oder oberen Schwellenwert oder beide an.
- Benachrichtigungen beschreiben, auf welche Weise und wohin Warnmeldungen zu senden sind, wenn die Schwellenwerte nicht erreicht werden.
- Durch die Kombination von Schwellenwerten und Benachrichtigungen erstellen Sie Warnmeldungen auf Basis der angegebenen Häufigkeit.
- Wenn automatische Warnmeldungen aktiviert sind (sie sind es standardmäßig), können Sie eine Policy erstellen und aktivieren, ***ohne*** Schwellenwerte festzulegen. Bei Aktivierung von automatischen Benachrichtigungen werden diese gesendet, wenn eine Ereignisquelle in der Gruppe um das angegebene Maß über oder unter der Baseline liegt.

Beispiel: Nehmen wir an, Sie haben eine Ereignisquellengruppe erstellt, die Ihre gesamten Windows-Ereignisquellen im Vereinigten Königreich umfasst. Sie können in diesem Beispiel eine Richtlinie angeben, die Ihnen jedes Mal eine Warnmeldung sendet, wenn weniger als 1000 Ereignisse innerhalb von 30 Minuten eingehen.

Hinweis: Zusätzlich zu oder anstelle der Einrichtung von Überwachungsrichtlinien für Ihre Ereignisquellengruppen können Sie Konfigurieren von automatischen Warnmeldungen, um Alarme anzuzeigen,wenn die Anzahl der Meldungen für eine Ereignisquelle außerhalb der normalen Grenzen liegt.

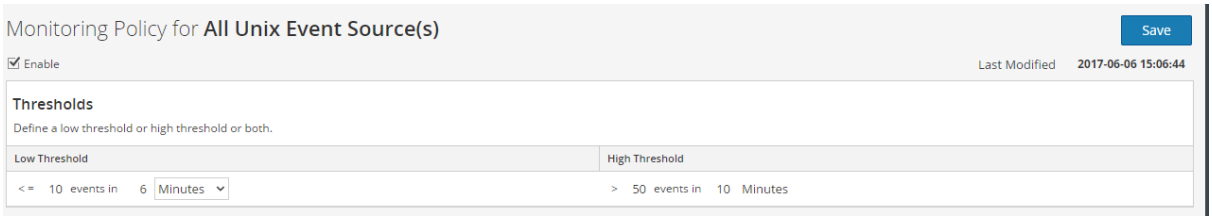
Konfigurieren von Warnmeldungen für Ereignisquellengruppen

Für jede Ereignisquellengruppe kann eine eigene Warnmeldungsrichtlinie erstellt werden. Dazu zählen die Festlegung von Schwellenwerten für das Erzeugen einer Warnmeldung oder die Festlegung des Benachrichtigungstyps bei Auslösung einer Warnmeldung. In diesem Thema werden die Schritte für die Erstellung einer Warnmeldungsrichtlinie für eine Ereignisquellengruppe beschrieben.

Erstellen einer Warnmeldungsrichtlinie für eine Ereignisquellengruppe

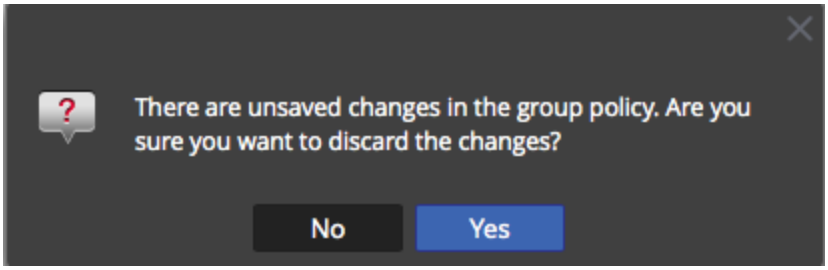
1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Überwachungsrichtlinien** aus.
3. Wählen Sie im Bereich **Ereignisgruppen** eine Gruppe aus.
4. Füllen Sie die Felder „Unterer Schwellenwert“ und „Oberer Schwellenwert“ aus.

Dies ist ein Beispiel für Schwellenwerte von Warnmeldungen.



5. Wählen Sie **Aktivieren** und klicken Sie auf **Speichern**, um die soeben konfigurierte Warnmeldungsrichtlinie zu aktivieren.

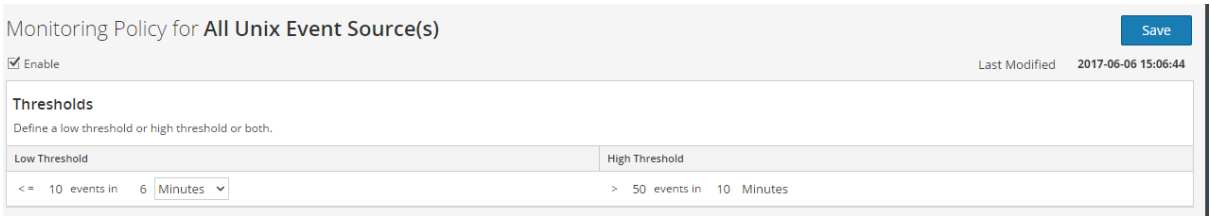
Hinweis: Wenn Sie an einer Richtlinie Änderungen vornehmen und die Seite verlassen möchten, ohne die Änderungen zu speichern, erscheint eine Warnmeldung, die Sie auf ungespeicherte Änderungen hinweist:



Einstellen und Anzeigen der Schwellenwerte einer Warnmeldungsrichtlinie

Jede Ereignisquellengruppe ist auch eine Warnmeldungsrichtlinie. Schwellenwerte sind Teil einer Warnmeldungsrichtlinie. Sie können Schwellenwerte für jede Warnmeldungsrichtlinie einstellen. Für jede Richtlinie können Sie einen unteren oder einen oberen Schwellenwert oder beides einstellen. Darüber hinaus können Sie eine Policy aktivieren, ohne Schwellenwerte festzulegen. So können Sie Benachrichtigungen basierend auf automatischen Warnmeldungen erhalten. Automatische Warnmeldungen werden erzeugt, wenn die Baseline für eine Ereignisquelle außerhalb der normalen Begrenzung liegt.

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Überwachungsrichtlinien** aus.
3. Wählen Sie im Bereich **Ereignisgruppen** eine Gruppe aus.
   Alle für eine ausgewählte Gruppe eingestellten Schwellenwerte werden im Bereich **Schwellenwerte** angezeigt.



4. Bearbeiten Sie die Werte für den unteren oder den oberen Schwellenwert wie folgt:

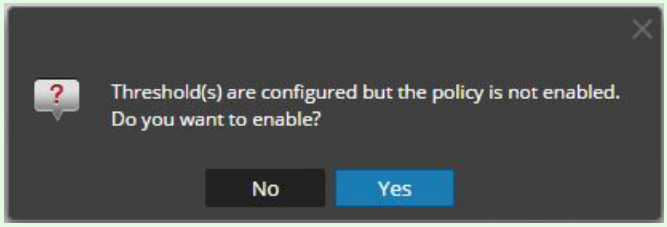
a. Geben Sie die Anzahl der Ereignisse für den Schwellenwert ein.

b. Geben Sie die Anzahl der Minuten oder Stunden für den Schwellenwert ein. Der Mindestwert ist 5 Minuten.

Hinweis: Für jeden Schwellenwert können Sie entweder die unteren Werte, die oberen Werte oder beides einstellen.

5. Wählen Sie **Aktivieren** aus, um Alarme zu aktivieren, wenn Schwellenwerte nicht erreicht werden.

Hinweis: Wenn Sie einen Schwellenwert konfigurieren und versuchen, die Seite zu speichern, ohne diesen zu aktivieren, werden Sie in einer Bestätigungsmeldung gefragt, ob die Policy aktiviert werden soll oder nicht:



Beispiel: Angenommen, Sie geben 10 und 30 als Werte für den unteren Schwellenwert ein: `10 events in 30 minutes`, und 20 und 30 als Werte für den oberen Schwellenwert: `20 events in 30 minutes`. Das bedeutet, dass Sie erwarten, dass zwischen 10 und 20 Ereignisse in 30 Minuten protokolliert werden (für die ausgewählte Ereignisquellengruppe). In diesem Fall werden alle Werte zwischen dem unteren und dem oberen Schwellenwert als normal betrachtet und lösen keinen Alarm aus.

Hinweis: Sobald Sie einer Richtlinie einen Schwellenwert hinzugefügt haben, können Sie ihn nicht mehr löschen. Sie können die Richtlinie deaktivieren oder Sie können den unteren oder oberen Schwellenwert auf 0 Ereignisse in 5 Minuten einstellen. Fünf Minuten ist die Mindestdauer für einen Schwellenwert.

Einrichten von Benachrichtigungen

In diesem Thema wird das Konfigurieren von Benachrichtigungen für Ereignisquellengruppen beschrieben. Benachrichtigungen werden gesendet, wenn Schwellenwerte überschritten werden.

Benachrichtigungen und Schwellenwerte sind eng verknüpft. Bevor Sie Benachrichtigungen konfigurieren, sollten Sie Schwellenwerte für eine Ereignisquellengruppe festlegen.

Hinweis: Wenn Sie nach dem Konfigurieren der Schwellenwerte für eine Ereignisquellengruppe keine Benachrichtigungen einrichten, werden die Benutzer nicht informiert, auch wenn ein Alarm ausgelöst wird. Allerdings sind alle Alarme auf der Registerkarte „Alarme“ sichtbar.

Voraussetzungen

Bevor Sie Benachrichtigungen für eine Ereignisquellengruppe einrichten, sollten Sie sich über die verfügbaren Benachrichtigungselemente informieren:

- **Benachrichtigungsserver:** Dies sind die Server, die Benachrichtigungen vom System erhalten sollen. Weitere Details finden Sie im Thema **Übersicht über Benachrichtigungsserver** im *Systemkonfigurationsleitfaden*.
- **Benachrichtigungsvorlagen:** Dies sind die verfügbaren Vorlagen für jeden Benachrichtigungstyp. Für das Ereignisquellenmanagement werden Standardvorlagen für E-Mail (SMTP), SNMP und Syslog bereitgestellt. Sie können die Vorlagen wie bereitgestellt verwenden, oder sie bei Bedarf anpassen. Weitere Details finden Sie im Thema **Vorlagenübersicht** im *Systemkonfigurationsleitfaden*.
- **Benachrichtigungsausgabe:** Die Ausgabe enthält die Parameter für den Benachrichtigungstyp. Beispiel: Eine E-Mail-Benachrichtigung enthält die E-Mail-Adressen und den Betreff für die Benachrichtigung. Weitere Details finden Sie im Thema **Benachrichtigungsausgaben – Übersicht** im *Systemkonfigurationsleitfaden*.

Hinzufügen von Benachrichtigungen zu einer Ereignisquellengruppe

So fügen Sie einer Ereignisquellengruppe Benachrichtigungen hinzu:

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Überwachungsrichtlinien** aus.
3. Wählen Sie im Bereich **Ereignisgruppen** eine Gruppe aus.

   Hinweis: Sie sollten bereits einen Schwellenwert für die Gruppe festgelegt haben. Wenn nicht, lesen Sie unter Einstellen und Anzeigen der Schwellenwerte einer Warnmeldungsrichtlinie die Informationen zum Festlegen eines Schwellenwerts und fahren Sie dann mit diesem Verfahren fort. Alternativ, wenn Sie automatische Warnmeldungen eingeschaltet haben, müssen Sie keine Schwellenwerte für eine Richtlinie festlegen. Automatische Alarme erzeugen Benachrichtigungen ohne die Notwendigkeit, Schwellenwerte festzulegen.

4. Klicken Sie im Bereich „Benachrichtigungen“ auf + und wählen Sie im Drop-down-Menü den Typ der hinzuzufügenden Benachrichtigung aus:
   - E-Mail
   - SNMP
   - Syslog

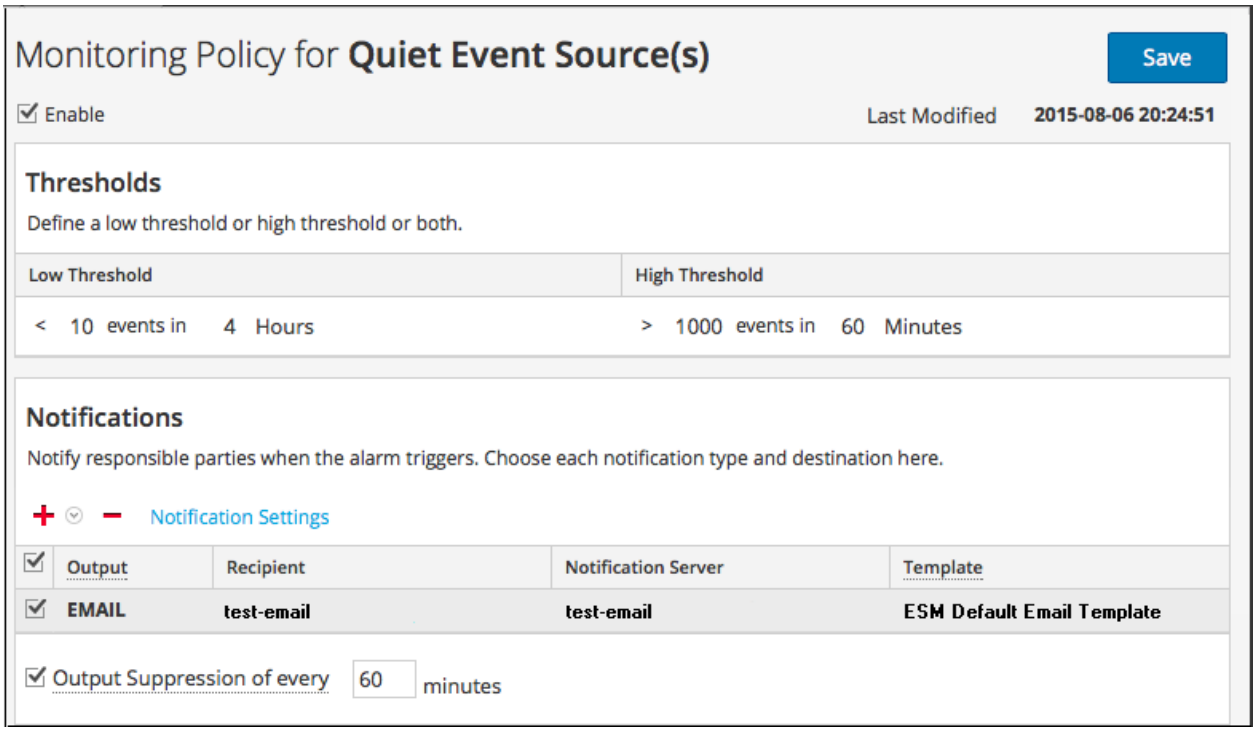
   Hinweis: Standardvorlagen für die ESM (Ereignisquellenüberwachung) werden für jeden Benachrichtigungstyp bereitgestellt.

5. Geben Sie Werte in die Felder „Benachrichtigung“, „Benachrichtigungsserver“ und „Vorlage“ ein.
   a. Wählen Sie den Wert für „Benachrichtigung“ in der Liste aus oder fügen Sie unter **Benachrichtigungen** einen passenden Benachrichtigungstyp hinzu und wählen Sie ihn dann hier aus.
   b. Wählen Sie den Wert für „Server“ in der Liste aus oder fügen Sie unter **Benachrichtigungen** einen passenden Server hinzu und wählen Sie ihn dann hier aus.
   c. Wählen Sie den Wert für „Vorlage“ in der Liste aus oder fügen Sie unter **Benachrichtigungen** eine passende Vorlage hinzu und wählen Sie sie dann hier aus.

Hinweis: Wenn Sie eines dieser Elemente hinzufügen oder bearbeiten möchten, klicken Sie auf **Benachrichtigungseinstellungen**. Auf der Seite **Administration > System > Globale Benachrichtigungen** wird ein neues Browserfenster geöffnet. Verwenden Sie diese Seite, um die verfügbaren Benachrichtigungselemente anzuzeigen oder zu aktualisieren.

6. Optional können Sie die Häufigkeit der Benachrichtigungen zu einer Richtlinie begrenzen.
   a. Wählen Sie **Ausgabeunterdrückung** aus, um eine Grenze festzulegen.
   b. Geben Sie einen Wert in Minuten für die Ausgabeunterdrückung an. Beispiel: Wenn Sie **30** eingeben, werden die Benachrichtigungen zu dieser Richtlinien auf eine Benachrichtigung alle 30 Minuten beschränkt.
   c. Klicken Sie auf **Speichern**.

Hier sehen Sie ein Beispiel für eine Überwachungsrichtlinie, die einen Schwellenwert und eine Benachrichtigung für eine Ereignisquellengruppe enthält.



Deaktivieren von Benachrichtigungen

Benachrichtigungen werden gesendet, wenn Schwellenwerte nicht erreicht werden. Darüber hinaus werden automatische Benachrichtigungen versendet, wenn Baselines nicht erfüllt werden. Sie können jedoch festlegen, dass Sie keine Benachrichtigungen für die Ereignisquellen in einer bestimmten Gruppe mehr benötigen. In diesem Fall können Sie die Benachrichtigungen für die Ereignisquellengruppe deaktivieren.

Hinweis: Selbst wenn Sie alle Benachrichtigungen deaktivieren, sind die Details für Alarme nach wie vor auf der Registerkarte „Alarme“ sichtbar.

Voraussetzungen

Sie müssen Schwellenwerte und Benachrichtigungen für eine Ereignisquellengruppe konfiguriert und aktiviert haben. Für automatische Benachrichtigungen müssen Sie die Option **Benachrichtigungen über automatische Überwachung aktivieren** auf der Registerkarte „Alarme“ ausgewählt haben.

Deaktivieren von Benachrichtigungen

So deaktivieren Sie Benachrichtigungen (sowohl manuelle als auch automatische) für eine Ereignisquellengruppe:

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Überwachungsrichtlinien** aus.
3. Wählen Sie im Bereich **Ereignisgruppen** eine Gruppe aus.
4. Klicken Sie auf **Aktivieren**, um das Häkchen zu entfernen. Das Löschen dieser Option bedeutet, dass für diese Ereignisquellengruppe keine Benachrichtigungen versendet werden, auch dann nicht, wenn Schwellenwerte nicht erreicht oder überschritten werden.
5. Zusätzlich können Sie alle Benachrichtigungen entfernen. Allerdings ist dies nicht erforderlich, um die Benachrichtigungen zu stoppen.

Zusätzliche Verfahren

Konfigurieren von automatischen Warnmeldungen

Hinweis: Automatische Warnmeldungen und ihre Einstellungen befinden sich derzeit im Betatest.

Voraussetzungen

Bevor Sie Benachrichtigungen für eine Ereignisquellengruppe einrichten, sollten Sie sich über die verfügbaren Benachrichtigungselemente informieren:

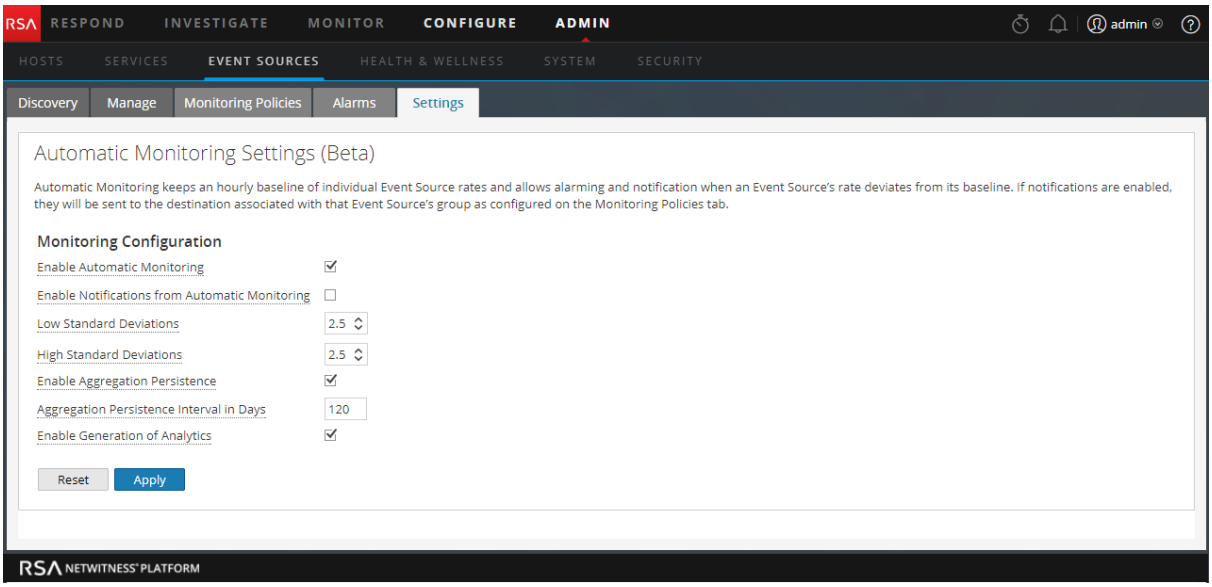
- **Benachrichtigungsserver:** Dies sind die Server, die Benachrichtigungen vom System erhalten sollen. Weitere Details finden Sie im Thema **Übersicht über Benachrichtigungsserver** im *Systemkonfigurationsleitfaden*.
- **Benachrichtigungsvorlagen:** Dies sind die verfügbaren Vorlagen für jeden Benachrichtigungstyp. Für das Ereignisquellenmanagement werden Standardvorlagen für E-Mail (SMTP), SNMP und Syslog bereitgestellt. Sie können die Vorlagen wie bereitgestellt verwenden, oder sie bei Bedarf anpassen. Weitere Details finden Sie im Thema **Vorlagenübersicht** im *Systemkonfigurationsleitfaden*.
- **Benachrichtigungsausgabe:** Die Ausgabe enthält die Parameter für den Benachrichtigungstyp. Beispiel: Eine E-Mail-Benachrichtigung enthält die E-Mail-Adressen und den Betreff für die Benachrichtigung. Weitere Details finden Sie im Thema **Benachrichtigungsausgaben – Übersicht** im *Systemkonfigurationsleitfaden*.

Konfigurieren von automatischen Warnmeldungen

So konfigurieren Sie automatische Warnmeldungen:

1. Navigieren Sie zu **ADMINISTRATION > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Einstellungen** aus.

   Die Registerkarte „Einstellungen“ wird angezeigt.



3. Standardmäßig ist die automatische Überwachung eingeschaltet. Deaktivieren Sie die Option **Automatische Überwachung aktivieren**, um automatische Warnmeldungen auszuschalten.
4. Standardmäßig sind Benachrichtigungen für automatische Warnmeldungen deaktiviert. Wählen Sie, um die automatischen Benachrichtigungen zu aktivieren, die Option **Benachrichtigungen von der automatischen Überwachung aktivieren** aus.
5. Konfigurieren Sie die Parameter basierend auf Ihren Nutzungsmustern:
   - **Untere Standardabweichungen**: Bei Unterschreitung dieser Standardabweichungen erhalten Sie Warnmeldungen. Der Standardwert ist **2.5** (Wahrscheinlichkeit von 95 %).
   - **Obere Standardabweichungen**: Bei Überschreitung dieser Standardabweichungen erhalten Sie Warnmeldungen. Der Standardwert ist **2.5** (Wahrscheinlichkeit von 95 %).

   Hinweis: Sie können die Einstellungen für die Standardabweichung in Schritten von 0,1 (ein Zehntel) einer Standardabweichung anpassen.
6. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen und die Einstellungen zu speichern.

Anzeigen von Ereignisquellenalarmen

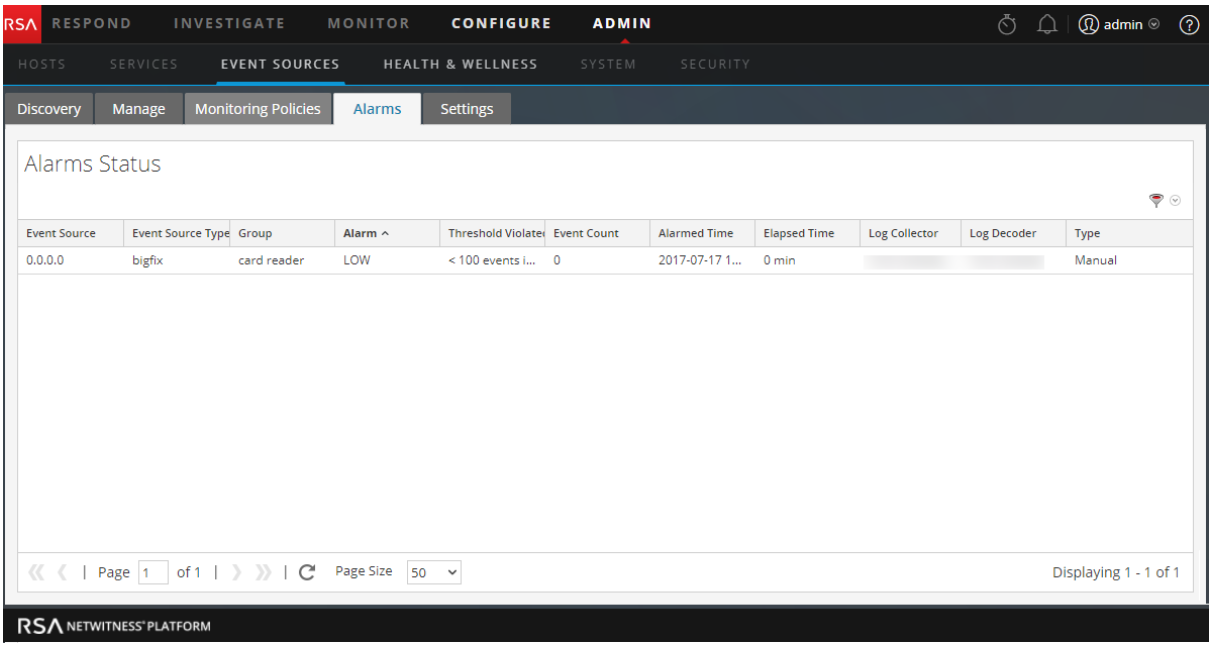
In diesem Thema wird beschrieben, wie Sie Alarme für Ihre Ereignisquellengruppen anzeigen können. Sobald Sie Warnmeldungen konfiguriert und festgelegt haben, können Sie alle generierten Alarme in der Registerkarte **Alarme** in der Ansicht **Ereignisquellen** anzeigen.

Alarminformationen sortieren

Wenn Sie das erste Mal auf diese Ansicht zugreifen, sind die Daten nach dem neuesten Alarm sortiert (die Spalte „Zeitpunkt des Alarms“). Sie können nach jeder beliebigen Spalte sortieren.

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Bewegen Sie den Cursor über eine Spalte, die Sie sortieren möchten.
3. Klicken Sie auf die Registerkarte **Alarme**.
4. Bewegen Sie den Cursor über die Spalte, die Sie sortieren möchten, und klicken Sie auf das Symbol ⬇.

   Dies ist ein Beispiel dafür, wenn Sie den Cursor über die Spalte „Alarm“ bewegen.



5. Wählen Sie entweder **Aufsteigend sortieren** oder **Absteigend sortieren** aus, um die Spalte so zu sortieren, wie Sie möchten.

   Die Daten werden auf allen Seiten sortiert.

Hinweis: Sie können auch nach zwei Spalten sortieren. Um dies zu erreichen, sortieren Sie zuerst nach der zweiten Spalte und dann nach der ersten Spalte. Beispiel: Wenn Sie alle HOHEN Alarme nach ihrer Gruppenreihenfolge anzeigen möchten, sortieren Sie zuerst **Gruppe** und sortieren Sie dann **Alarm**.

Warnmeldungen nach Typ filtern

Sie können die Alarme auch nach ihrem Typ filtern: Sie können entweder nur die manuellen oder nur die automatischen (Baseline-) Alarme anzeigen. Wählen Sie, um nach Alarmtyp zu filtern, das Filtersymbol auf der rechten Seite des Bildschirms im Bereich der Überschrift aus:

Wählen Sie entweder „Automatisch“ oder „Manuell“ aus:

- Wenn Sie „Automatisch“ auswählen, werden nur die Warnmeldungen basierend auf Baselines angezeigt.
- Wenn Sie „Manuell“ auswählen, werden nur die Alarme angezeigt, für die Sie Schwellenwerte festgelegt haben.

Referenzen für das Ereignisquellenmanagement

Folgende Themen enthalten Referenzinformationen für das Ereignisquellenmanagement:

- Registerkarte „Erkennung“
- Registerkarte „Managen“
- Registerkarte „Ereignisquelle verwalten“
- Ansicht „Ereignisquellen“
- Erstellen/Bearbeiten von Gruppenformularen
- Detailansicht
- Parser-Zuordnungen verwalten
- Registerkarte „Alarme“
- Registerkarte Überwachungsrichtlinien
- Registerkarte „Einstellungen“

Registerkarte „Erkennung“

Um auf die Registerkarte „Erkennung“ zuzugreifen, navigieren Sie zu NetWitness ADMIN> Ereignisquellen. Die Registerkarte „Erkennung“ wird angezeigt.

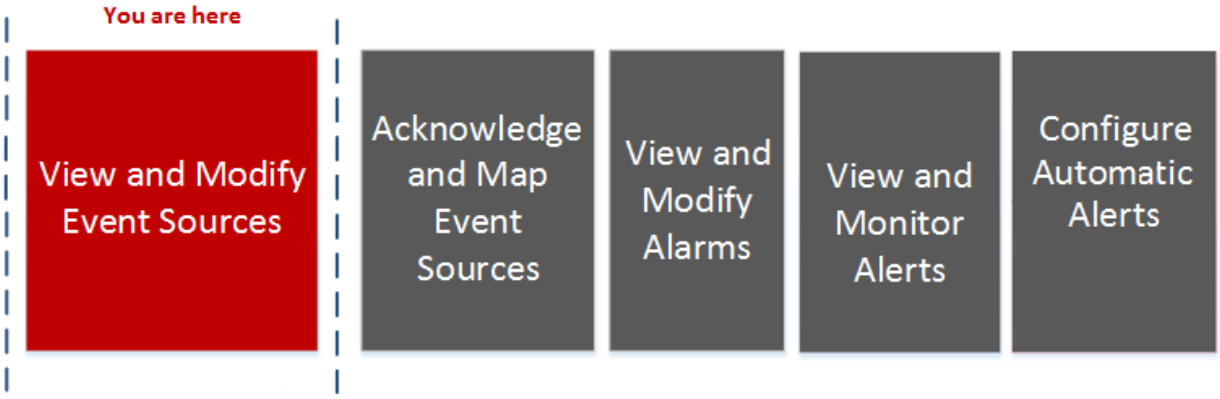
Auf der Registerkarte „Erkennung“ sehen Sie alle Ereignisquellen, die NetWitness unter den einzelnen Adressen erkannt hat, samt Angaben zu ihrem Typ und der Wahrscheinlichkeit, mit der das System sie vollständig korrekt identifiziert hat. Wenn die erkannten Ereignisquellentypen korrekt sind, können Sie bestätigen, dass die betreffende Ereignisquelle herausgefiltert werden soll. Wenn sie falsch sind, können Sie die zulässigen Ereignisquellentypen für eine bestimmte Adresse festlegen, damit zukünftige Protokolle mit dem richtigen Parser analysiert werden.

Hinweis: Die folgenden Funktionen gelten für RSA NetWitness® Platform Version 11.1 und höher:
- Bestätigung mehrerer Ereignisquellen
- Filterung nach Ereignisquelltyp
- (für 11.2 und höher) Zuordnungsfilteroptionen „Keine“, „Automatisch“ und „Manuell“
- Zuordnung mehrerer Ereignisquellen
- Suche nach Ereignisquellen auf der Seite „Ereignisquellenerkennung“

RSA NetWitness® Platform in der Version11.2 und höher ordnet eingehende Ereignisse automatisch anhand früherer Protokolle, die von dieser Adresse erhalten wurden, einem Typ zu und reduziert damit das nicht korrekte Parsing von Nachrichten sowie die Anzahl der Elemente, für die Ihre Aufmerksamkeit im Erkennungsworkflow erforderlich ist. Der Wert **Automatisch** in der Spalte **Zuordnungstyp** gibt an, dass eine Adresse automatisch zugewiesen wurde.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Bestätigen und Zuordnen von Ereignisquellen.*	Bestätigen und Zuordnen von Ereignisquellen

Rolle	Ziel	Dokumentation
Administrator	Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.*	Parser-Zuordnungen verwalten
Administrator	Anzeigen von Ereignisquellenalarmen.	Anzeigen von Ereignisquellenalarmen
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

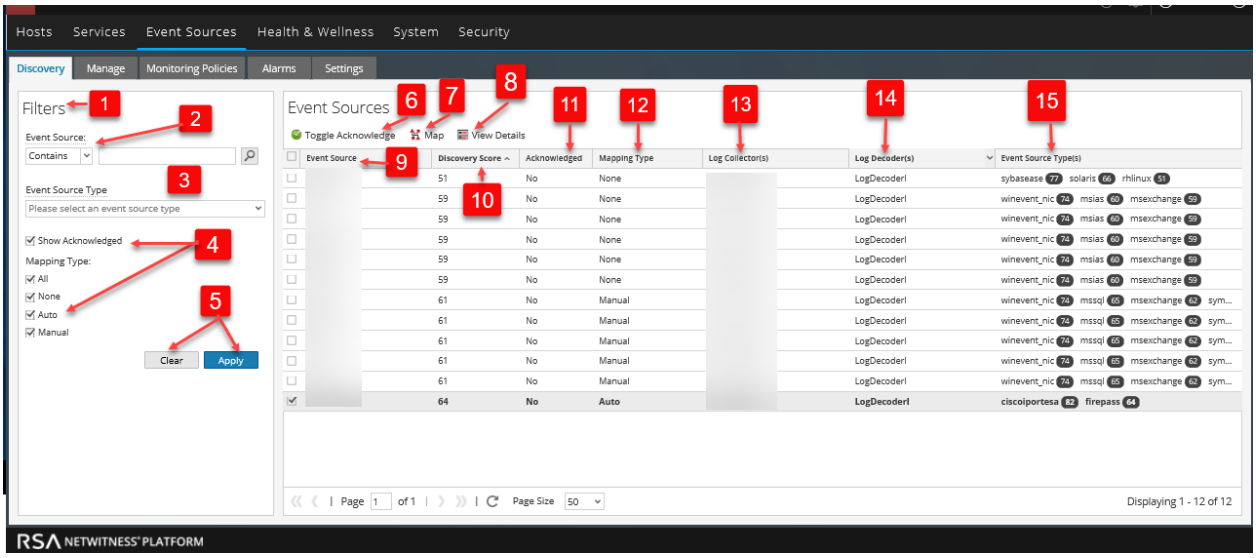
Parser-Zuordnungen verwalten

Detailansicht

Überblick

Das Beispiel unten zeigt eine Liste mit Adressen und den für sie erkannten Ereignisquellentypen. Unter „Ereignisquellentypen“ werden alle Ereignisquellen aufgeführt, die erkannt wurden.

Dies ist ein Beispiel für die Registerkarte.



1 Zeigt die Bereiche „Filter“ und „Ereignisquellen“ mit geöffneter Registerkarte „Erkennung“ an.

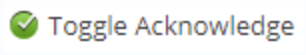
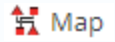
2 Zeigt das Feld „Ereignisquellenfilter“ mit einem Drop-down-Menü an, das folgende Optionen bietet:

- Geben Sie die vollständige oder einen Teil der Adresse (IP, IPv6 oder Hostname) der Quelle (n) ein, die Sie überprüfen möchten. Sie können auch mehrere Einträge eingeben, die durch Kommas getrennt sind.
  Beispiel: **10.10.10.10,10.10.10.11,host1.company.com**
- **Exakt:** Gibt Quellen zurück, die vollständig mit dem Suchbegriff übereinstimmen.
  Beispiel: **10.10.10.10** gibt nur **10.10.10.10** und nicht **10.10.10.101** zurück.

	• **Beginnt mit:** Gibt Quellen zurück, die mit dem Suchbegriff beginnen. Beispiel: **10.10.10.** gibt das gesamte **10.10.10.x Subnetz** zurück. • **Enthält:** Gibt Quellen zurück, die mit dem Suchbegriff beginnen. Beispiel: **exch** gibt Begriffe wie **us-exch-1.company.com** zurück oder **lab21** gibt Begriffe wie **hostx.lab21.company.com** zurück. • **Endet mit:** Gibt Quellen zurück, die mit dem Suchbegriff enden. Beispiel: **lab21.company.com** gibt alle Hosts zurück. **Hinweis:** Wenn Sie den Suchtext eingeben, können Sie die Zeichen **. - :** (Punkt, Strich, Doppelpunkt) verwenden.
3	Mit dem Drop-down-Menü „Ereignisquellentyp“ können Sie nach Adressen filtern, die alle ausgewählten Ereignisquellentypen enthalten.
4	• Aktivieren Sie das Kontrollkästchen **Bestätigte anzeigen**, um die bestätigten Ereignisquellen anzuzeigen. • Die Filteroptionen für die Zuordnung können nur einen der im Filterbereich aufgelisteten Zuordnungstypen enthalten oder es können mehrere Zuordnungstypen ausgewählt werden. **Hinweis:** Wenn keine Filteroptionen für die Zuordnung ausgewählt sind, werden standardmäßig die Zuordnungstypen **Alle**, **Ohne**, **Manuell zugeordnet** und **Automatisch** angezeigt.
5	• Die Schaltfläche **Anwenden** verwendet alle Kriterien, die in allen Filtern festgelegt sind. • Die Schaltfläche **Löschen** löscht alle Filter im Bereich.
6	Schaltet zwischen bestätigten und nicht bestätigten Ereignisquellen um.
7	Ordnet die ausgewählten Ereignisquellen zu.
8	Schaltfläche „Details anzeigen“ zum Aufrufen von Details zu der ausgewählten Ereignisquelle
9	Zeigt die Adressen der ausgewählten Ereignisquellen an.
10	Zeigt den Discovery Score für die ausgewählten Ereignisquellen an.
11	Zeigt an, ob die ausgewählten Ereignisquellen bestätigt wurden oder nicht.
12	Zeigt den ausgewählten Typ der Ereignisquellenzuordnung als „Automatisch“, „Manuell zugeordnet“ oder „Ohne“ an. Änderungen an der Zuordnung werden nur hier angezeigt.
13	Zeigt die Hostnamen der Log Collector-Instanzen an, von denen die Ereignisquelle gehostet wird.
14	Zeigt die Hostnamen der Log Decoder-Instanzen an, von denen die Ereignisquelle gehostet wird.
15	Zeigt die erkannten Ereignisquellentypen samt ihres Discovery Score an.

Symbolleiste und Funktionen

Die Registerkarte „Erkennung“ enthält die folgenden Funktionen:

Feld	Beschreibung
Tools   	Folgende Optionen sind in der Symbolleiste verfügbar: • **Bestätigung umschalten**: Schaltet den Bestätigungsstatus für die ausgewählte Ereignisquelle zwischen **Ja** und **Nein** um. • **Karte**: Öffnet das Dialogfeld „Parser-Zuordnungen verwalten“, in dem Sie eine Ereignisquelle dem richtigen Protokollparser zuweisen können. • **Details anzeigen**: Enthält Details über die ausgewählte Ereignisquelle.
Ereignisquelle	Die IP-Adresse, IPv6-Adresse oder der Hostname der Ereignisquelle.
Discovery Score	Zeigt den allgemeinen Discovery Score der betreffenden Adresse an. Höhere Ergebnisse weisen auf ein stärkeres Vertrauen hin. Der Discovery Score kann einen Wert zwischen 0 (geringste Zuverlässigkeit) bis 100 (höchste Zuverlässigkeit) haben.
Bestätigt	Zur Auswahl stehen **Ja** (Sie haben die Ereignisquelle bestätigt) oder **Nein** (Sie haben die Ereignisquelle nicht bestätigt).

Feld	Beschreibung
Zuordnungstyp	Zur Auswahl stehen **Manuell zugeordnet** (Sie haben die Ereignisquelle zugewiesen), **Automatisch** (das System hat die Ereignisquelle automatisch zugewiesen) oder **Ohne** (Sie haben die Ereignisquelle nicht zugewiesen). Die automatische Zuordnung erfolgt inhaltsbezogen. Wenn es sich bei einer Protokollnachricht um eine Nachricht mit einem vertrauensvollen Header oder um eine Nachricht handelt, die mit Tags versehen wurde, wird für diese Adresse und diesen Typ eine automatische Zuordnung eingestellt. Diese automatische Zuordnung ist 24 Stunden gültig und wird jedesmal erneuert, wenn eine Protokollnachricht mit einem mit Tags versehenen Header einer Nachricht übereinstimmt. Protokollnachrichten werden zunächst anhand automatisch zugewiesener Parser analysiert und gehen nur dann zurück in die Erkennung, wenn sich unter den zugewiesenen Parsern keine Übereinstimmung findet. Protokollnachrichten, die zurück in die Erkennung gehen, können mit den mit Tags versehenen Headern oder Nachrichten anderer Ereignisquellen übereinstimmen. Dies führt dazu, dass mehrere Typen zugewiesen werden. Zum Beispiel könnte eine Adresse irgendwann auf Windows, MS SQL und Apache zugewiesen werden und diese Parser werden zuerst ausgewertet. Wird eine Ereignisquelle stillgelegt und ihre IP-Adresse erneut verwendet, werden die Zuordnungen für die stillgelegten Typen enstprechend dem 24-Stunden-Timer ungültig. **Hinweis:** Diese Funktion gilt für die RSA NetWitness Version 11.2 und höher.
Log Collector	Log Collector, die Protokolle von dieser Ereignisquellenadresse erhalten haben.
Log Decoder	Log Decoder, die Protokolle von dieser Ereignisquellenadresse erhalten haben.
Ereignisquelltyp(en)	Die analysierten Typen der Ereignisquellenadresse und der entsprechenden Discovery Score für jeden Typ.

Hinweis: Discovery Scores sind nur für Log Decoder ab Version 11.0 verfügbar. Discovery Scores für eine Log Decoder-Version vor 11.0 werden als „Nicht verfügbar“ angezeigt.

In der folgenden Tabelle wird die Sortierreihenfolge für Discovery Scores beschrieben. Um auf das Drop-down-Menü „Sortierreihenfolge“ zuzugreifen, klicken Sie auf den Pfeil nach unten in der Spalte „Ereignisquellen“.

Feld	Beschreibung
Aufsteigend sortieren	Sortiert die Spalte nach Discovery Score in aufsteigender Reihenfolge.
Absteigend sortieren	Sortiert die Spalte nach Discovery Score in absteigender Reihenfolge.
Spalten	Wird verwendet, um eine oder mehrere Spalten ein- oder auszublenden.

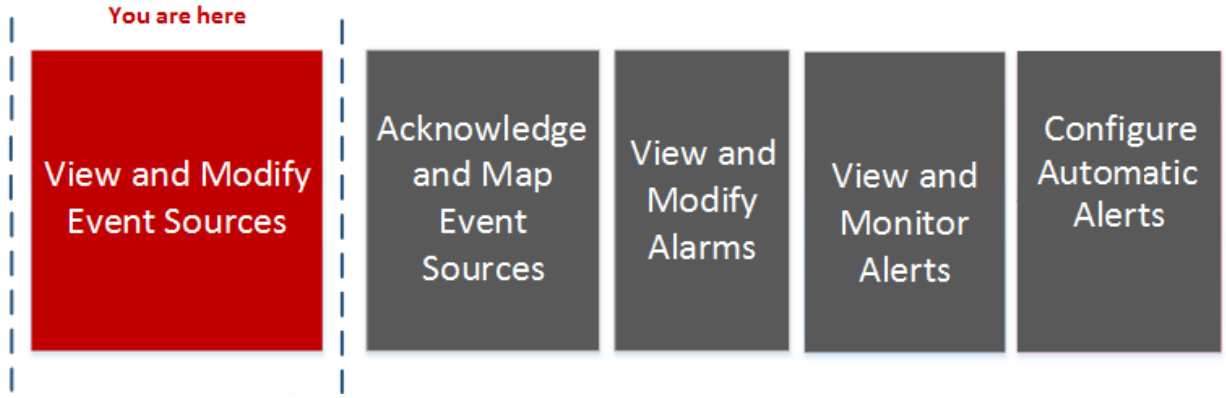
Registerkarte „Managen“

Die Registerkarte „Managen“ ordnet Ereignisquellen in Gruppen ein und zeigt für jede Ereignisquelle Attribute an.

Um auf diese Registerkarte zuzugreifen, navigieren Sie zu **ADMIN > Ereignisquellen > Managen**.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	* Anzeigen und Ändern von Ereignisquellen.	Managen von Ereignisquellengruppen
Administrator	Bestätigen und Zuordnen von Ereignisquellen.	Bestätigen und Zuordnen von Ereignisquellen
Administrator	Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.	Parser-Zuordnungen verwalten
Administrator	Anzeigen von Ereignisquellenalarmen.	Anzeigen von Ereignisquellenalarmen
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

*Sie können diese Aufgabe hier durchführen.

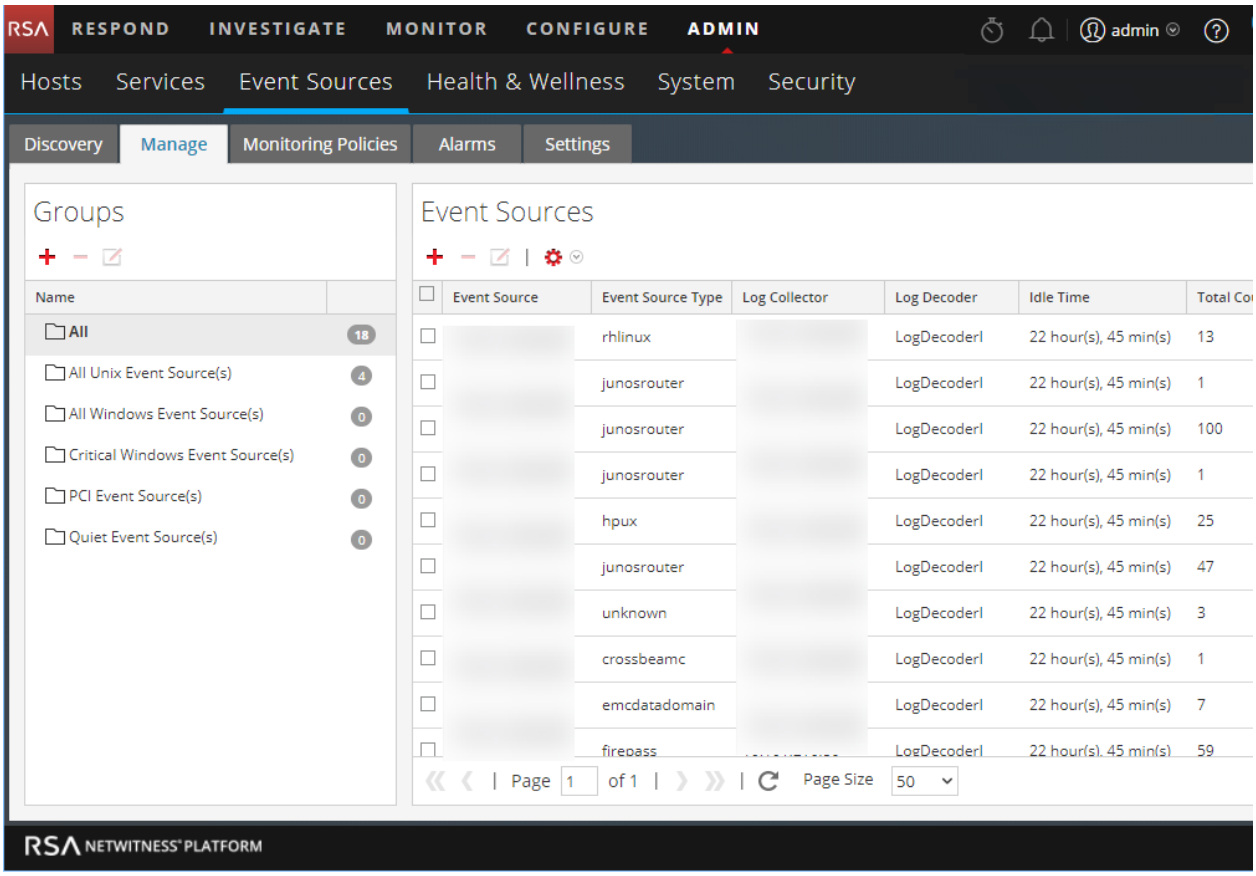
Verwandte Themen

Erstellen von Ereignisquellengruppen

Erstellen von Ereignisquellen und Bearbeiten von Attributen

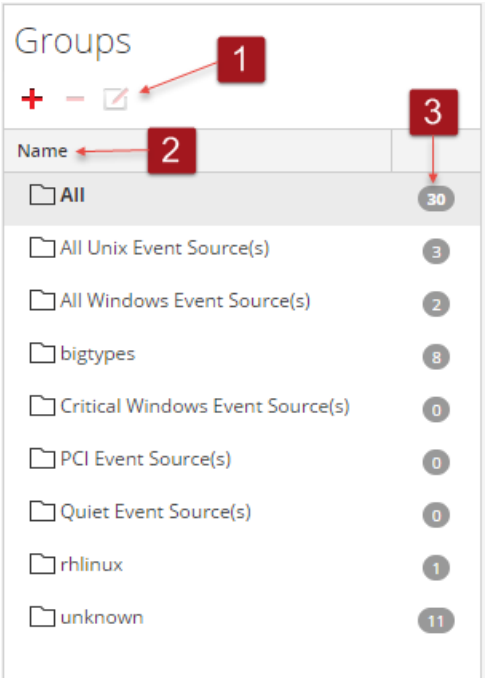
Überblick

Die Registerkarte „Managen“ ordnet Ereignisquellen in Gruppen ein und zeigt für jede Ereignisquelle Attribute an. Die Registerkarte „Managen“ besteht aus zwei Bereichen: „Gruppen“ und „Ereignisquellen“.



Bereich Gruppen

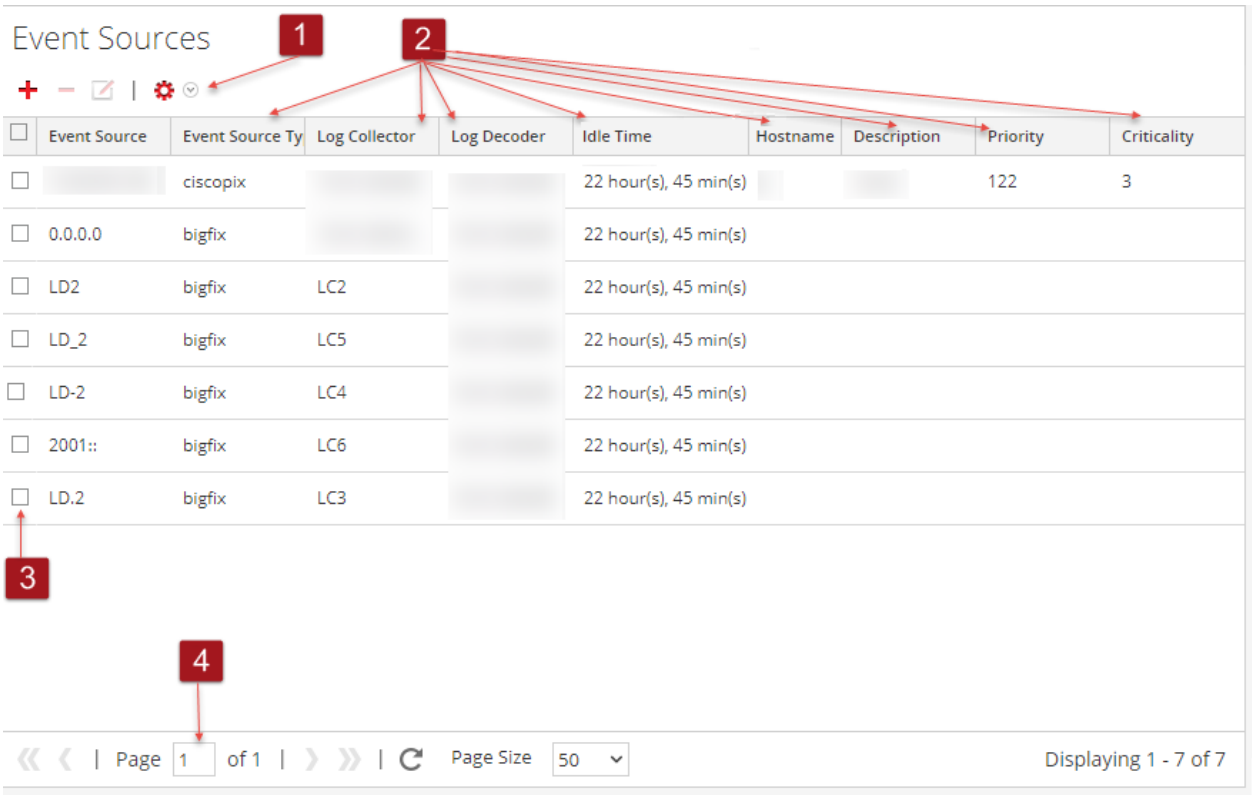
Der Gruppenbereich listet die Ereignisquellengruppen sowie die Anzahl der Mitglieder für jede Gruppe auf. Wählen Sie aus der Gruppenliste **Alle** aus, um alle Ereignisquellen anzuzeigen. Dies ist ein Beispiel für den Gruppenbereich.



1	Dies sind die NetWitness Platform-Standardsymbole für das Hinzufügen, Entfernen oder Bearbeiten von Gruppen.
2	In der Spalte „Name“ werden die Bezeichner der einzelnen Gruppen aufgeführt. Sie können mithilfe der Gruppennamen schnell einige der Kriterien erkennen, die für die Bildung der Gruppe verwendet wurden. Wenn Sie zum Beispiel eine Gruppe erstellen, die aus Windows-Ereignisquellen für die Vertriebsorganisation besteht, könnten Sie die Gruppe **Windows-Vertriebsquellen** nennen. **Hinweis:** Der Name der Ereignisquellengruppe kann nicht bearbeitet werden. Nachdem Sie eine Gruppe erstellt haben, besteht der Name so lange, wie die Gruppe selbst besteht.
3	Die Anzahl für eine Ereignisquellengruppe gibt an, wie viele Ereignisquellen sich in dieser Gruppe befinden. Das heißt, die Anzahl der Ereignisquellen, die den Kriterien entsprechen, die diese Gruppe definieren. **Hinweis:** Die Anzahl wird nicht dynamisch aktualisiert, wenn neue Ereignisquellen hinzugefügt werden. Daher müssen Sie manuell aktualisieren, wenn Sie eine aktualisierte Gruppenanzahl sehen möchten.

Ereignisquellenbereich

Der Ereignisquellenbereich zeigt die Attribute für die Ereignisquellen in der ausgewählten Gruppe an. Ist im Bereich „Gruppen“ die Option „Alle“ ausgewählt, werden im Bereich „Ereignisquellen“ sämtliche Ereignisquellen aufgeführt.



1 Die Symbolleiste enthält folgende Tools:

- **Hinzufügen**: eine Ereignisquelle manuell hinzufügen
- **Entfernen**: Eine Ereignisquelle entfernen
- **Bearbeiten**: Attribute für eine bestehende Ereignisquelle aktualisieren
- Menü **Importieren/Exportieren**: Zeigt ein Menü mit den folgenden Optionen an:
  - **Import**: Ereignisquellen aus einer Contentmanagementdatenbank (CMDB), einem Spreadsheet oder einem anderen Tool importieren.
  - **Exportieren**: Ausgewählte Ereignisquellen und ihre Attribute im CSV-Format exportieren.
  - **Gruppe exportieren**: Die gesamte aktuell ausgewählte Gruppe exportieren.

2 Spaltenanzeige der Attribute. Sie können wählen, welche Attribute angezeigt werden:

3 Kontrollkästchen: Wählen Sie zu verwendende Zeilen aus, wenn Sie Aufgaben auf mehrere Ereignisquellen anwenden möchten, etwa bei der Massenbearbeitung.

4 Navigationstools:

Unten auf dem Bildschirm finden Sie Elemente zur Navigation in Ihrer Gruppe:

- **Seite *x* von *y***: Zeigt an, welche Seite gegenwärtig angezeigt wird, und wie viele Seiten es für diese Gruppe insgesamt gibt.
- <<, <, > und >>: Klicken Sie auf diese Symbole, um sich zwischen Seiten zu bewegen, entweder jeweils eine weiter oder zurück (< und >) oder zur ersten (<<) oder zur letzten (>>) Seite.
- **Seitengröße**: Wählen Sie mit dieser Auswahl die Größe Ihrer Seite aus.
- ***x* - *y* von *z* werden angezeigt**: schnelle Prüfung, welche Ereignisquellen aus der Gesamtanzahl für die Gruppe gegenwärtig angezeigt werden.

Sortierung

Im Ereignisquellenbereich wird die Liste der Elemente in sortierter Reihenfolge präsentiert. Sie können wählen, nach welcher Spalte sortiert werden soll. Beachten Sie jedoch, dass die Sortierreihenfolge Groß- und Kleinschreibung unterscheidet.

Wenn die Werte in einer Spalte eine Mischung aus Klein- und Großbuchstaben enthält, werden die Werte mit Großbuchstaben vor denjenigen mit Kleinbuchstaben angezeigt.

Beispiel: Angenommen, die Spalte „Ereignisquelltyp“ enthält die folgenden Einträge: Netflow, APACHE, netwitnessspectrum, ciscoasa. Die Sortierreihenfolge wäre:

- APACHE
- Netflow
- ciscoasa
- netwitnessspectrum

Registerkarte „Ereignisquelle verwalten“

Der Bildschirm „Ereignisquelle verwalten“ verfügt über mehrere integrierte Komponenten, die eine Ereignisquelle aus unterschiedlichen Perspektiven darstellen.

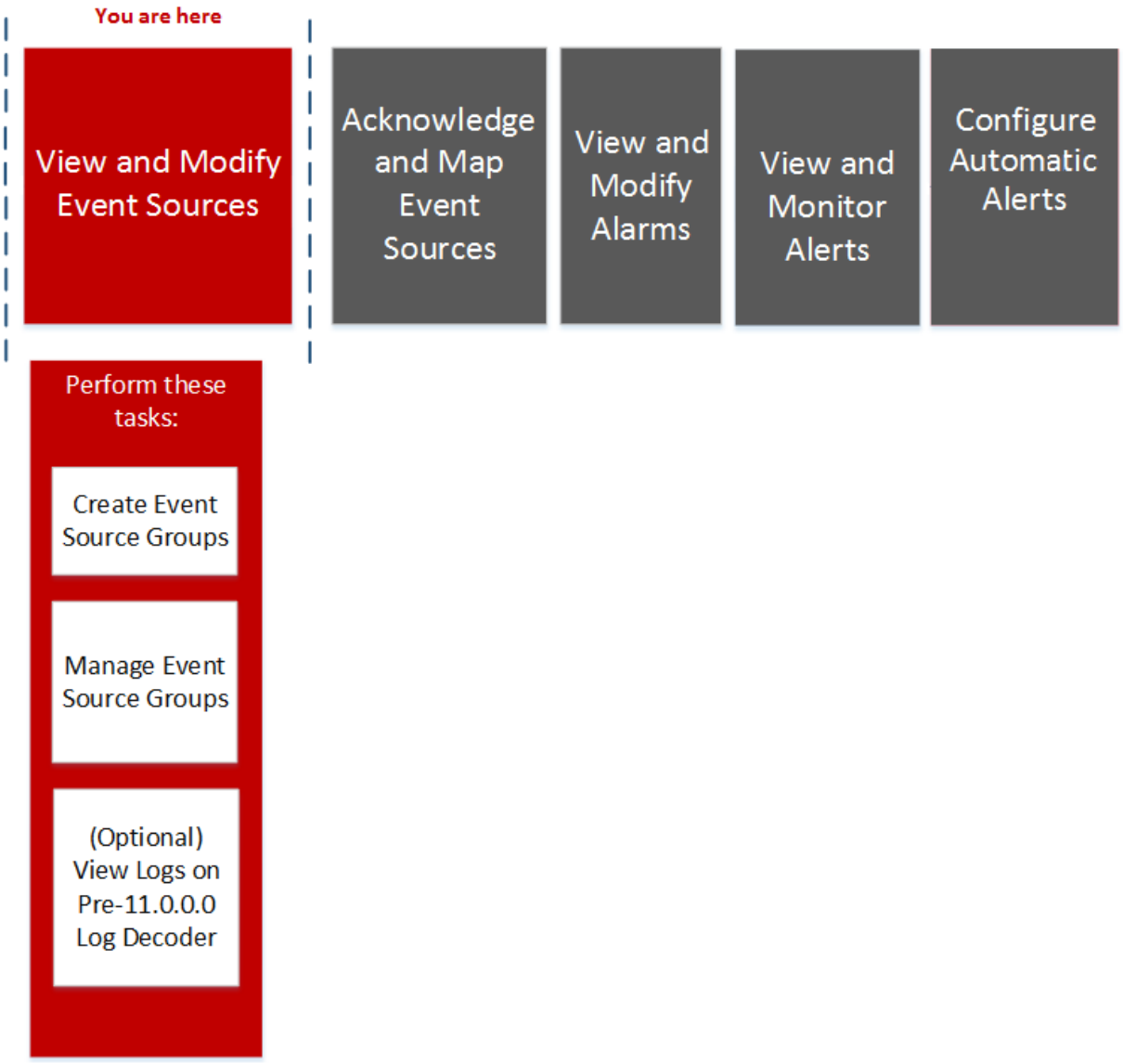
- Anzeigen von Ereignisquellendetails
- Hinzufügen von Attributwerten zu einer Ereignisquelle
- Entfernen von Attributwerten für eine Ereignisquelle

So zeigen Sie den Bildschirm „Ereignisquelle verwalten“ für eine Ereignisquelle an:

1. Navigieren Sie zu **ADMIN > Ereignisquellen**.
2. Wählen Sie die Registerkarte **Managen** aus.
3. Wählen Sie im Bereich „Ereignisquellen“ eine Ereignisquelle in der Liste aus und klicken Sie auf +.

Workflow

Dieser Workflow zeigt das End-to-End-Verfahren zum Ändern, Bestätigen, Zuordnen und Konfigurieren von Ereignisquellen, zusammen mit der Anzeige und Konfiguration von Ereignisquellenalarmen und zugehörigen Warnmeldungen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Ereignisquellengruppe erstellen, die alle Ereignisquellen mit hoher Priorität enthält	Erstellen von Ereignisquellengruppen
Administrator	Ereignisquellenattribute bearbeiten	Erstellen von Ereignisquellen und Bearbeiten von Attributen

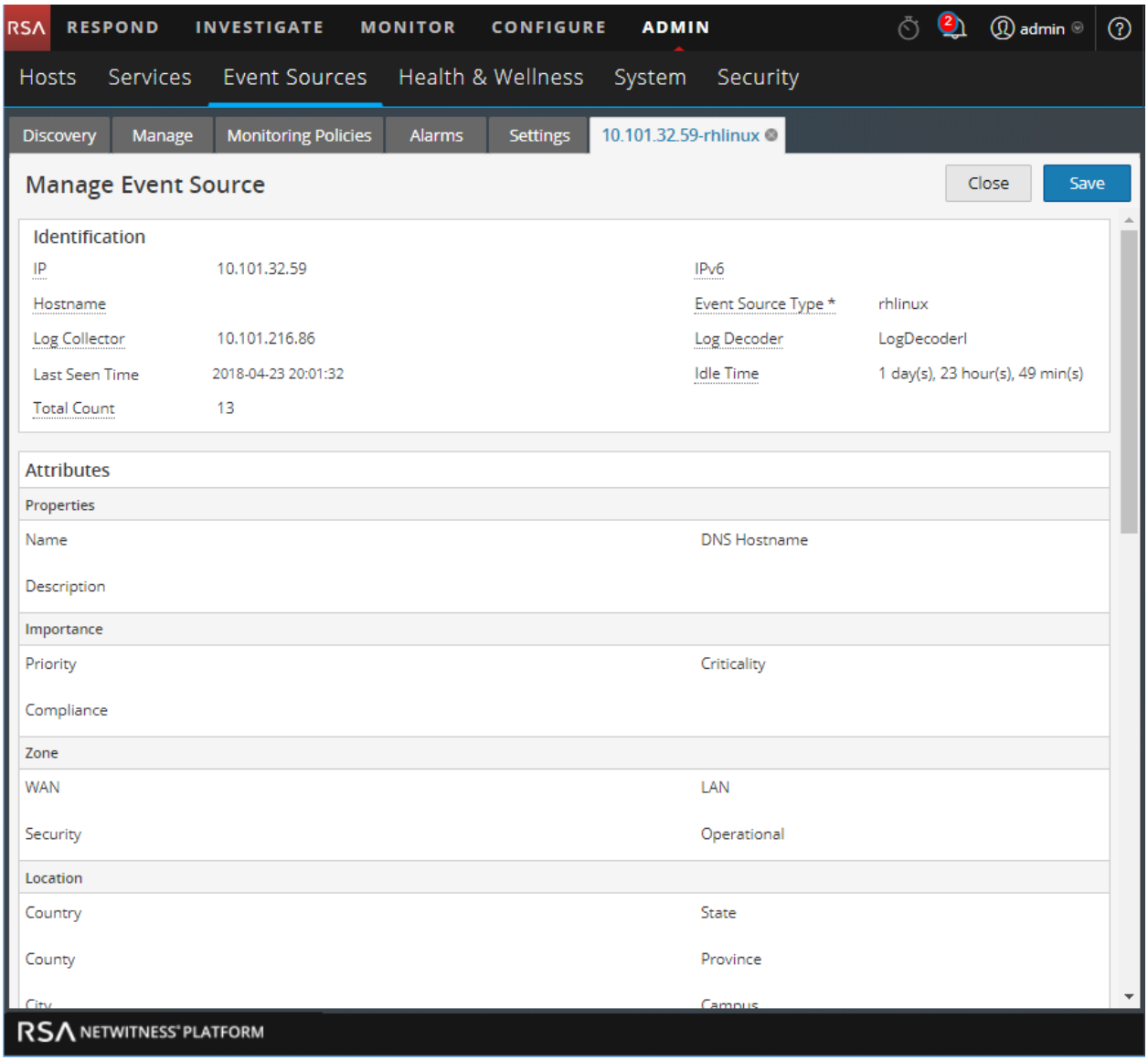
Verwandte Themen

Erstellen von Ereignisquellen und Bearbeiten von Attributen

Erstellen von Ereignisquellengruppen

Überblick

Dies ist ein Beispiel für die Registerkarte „Ereignisquelle“:



In dieser Tabelle werden die Kategorien für die Ereignisquellenattribute beschrieben.

Abschnitt der Attribute	Beschreibung
Identifizierung	Diese Attribute sind die Hauptattribute, die zusammen eine Ereignisquelle identifizieren. Diese Attribute können Sie nur ändern, wenn Sie die Details für eine neue Ereignisquelle angeben. Für eine existierende Ereignisquelle werden die Attribute in diesem Abschnitt automatisch aufgefüllt und können auf diesem Bildschirm nicht geändert werden. Attribute für eine neue Ereignisquelle: • IP • IPv6 • Hostname • Ereignisquellentyp • Log Collector • Log Decoder Folgende Attribute werden bei der Anzeige von Details für eine bestehende Ereignisquelle anzeigt: • „Zuletzt angezeigt“: Zeitpunkt, zu dem die Kommunikation zwischen NetWitness Platform und der Ereignisquelle angezeigt wurde • „Inaktivitätsdauer“: Das ist die Zeit, die seit **Zuletzt angezeigt** verstrichen ist. Diese Zeit kann nützlich sein, wenn Sie Ereignisquellen filtern wollen, die für eine bestimmte Dauer inaktiv waren. • „Gesamtanzahl“: Gesamtzahl aller Ereignisquellen für diesen **Ereignisquellentyp**.
Eigenschaften	Diese Attribute stellen den Namen und die Beschreibung bereit. • Name • DNS-Hostname • Beschreibung
Bedeutung	Diese Attribute können für eine Gruppierung nach Priorität verwendet werden. • Priorität • Bedeutung • Compliance

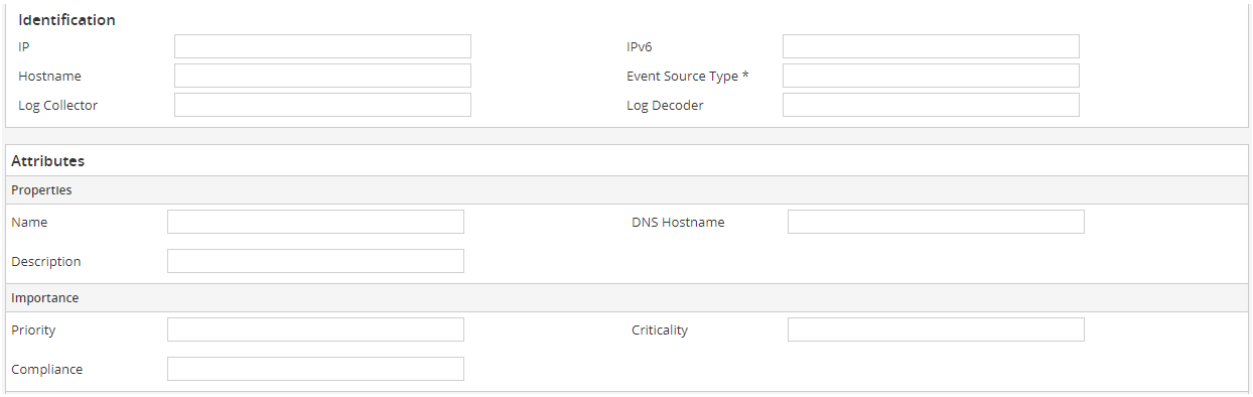
Abschnitt der Attribute	Beschreibung
Zone	Diese Attribute können für eine Gruppierung nach Zone verwendet werden. • WAN (Wide Area Network) • LAN (Local Area Network) • Sicherheit • Operational
Location	Diese Attribute können für eine Gruppierung nach physischem oder geografischem Standort verwendet werden. • Land • State • Kreis • Bundesland/Region • Stadt • Campus • Postal Code • Gebäude • Stockwerk • Raum
Organisation	Diese Attribute können für eine Gruppierung nach Organisation und für die Bereitstellung von Kontaktinformationen verwendet werden. • Unternehmen • Division • Geschäftsbereich • Abteilung • Gruppe • Ansprechpartner • Telefonnummer des Kontakts • E-Mail-Adresse des Kontakts

Abschnitt der Attribute	Beschreibung
Eigentümer	Diese Attribute geben die Verantwortlichen für die Ereignisquelle an. • Manager • Primärer Administrator • Backupadministrator
Physisch	Diese Attribute geben die physischen Eigenschaften für die Ereignisquelle an. • Anbieter • Seriennummer • Ressourcen-Tag • Voltage • USV-geschützt • Rackhöhe • Tiefe • BTU-Ausgabe • Farbe
Funktion	Diese Attribute können für eine Gruppierung nach Funktion verwendet werden. • Primäre Rolle • Unterrolle 1 • Unterrolle 2
Systeminformationen	Diese Attribute geben Systeminformationen an. • Domainname • System Name • Kennung • Systembeschreibung
Custom	Dieser Abschnitt bietet acht benutzerdefinierte Attribute für beliebige andere von Ihrer Organisation benötigte Attribute.

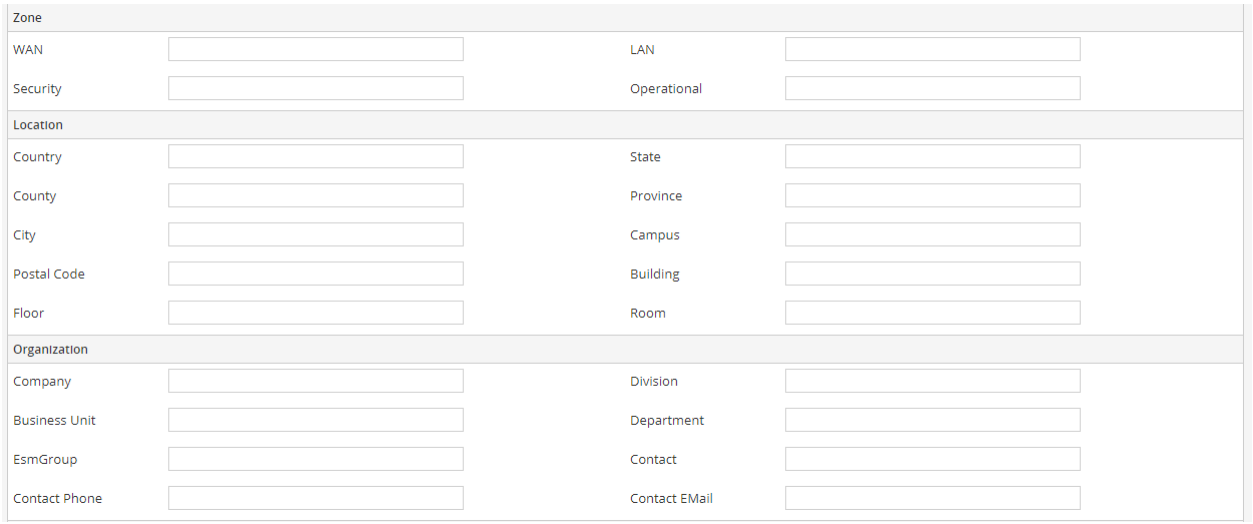
Funktionen

Die Einstellungen auf der Registerkarte Ereignisquelle verwalten sind eine Kombination von automatisch aufgefüllten Informationen und Eingaben der Benutzer. Wenn eine Ereignisquelle Protokollinformationen an NetWitness Platform sendet, wird sie der Liste der Ereignisquellen hinzugefügt und einige grundlegende Informationen werden automatisch ausgefüllt. Danach kann der Benutzer jederzeit Details zu anderen Ereignisquellenattributen hinzufügen oder bearbeiten.

Die folgende Abbildung zeigt ein Beispiel für die Abschnitte **Identifikation**, **Eigenschaften** und **Wichtigkeit**.



Diese Abbildung zeigt ein Beispiel für die Abschnitte **Zone**, **Standort** und **Organisation**.



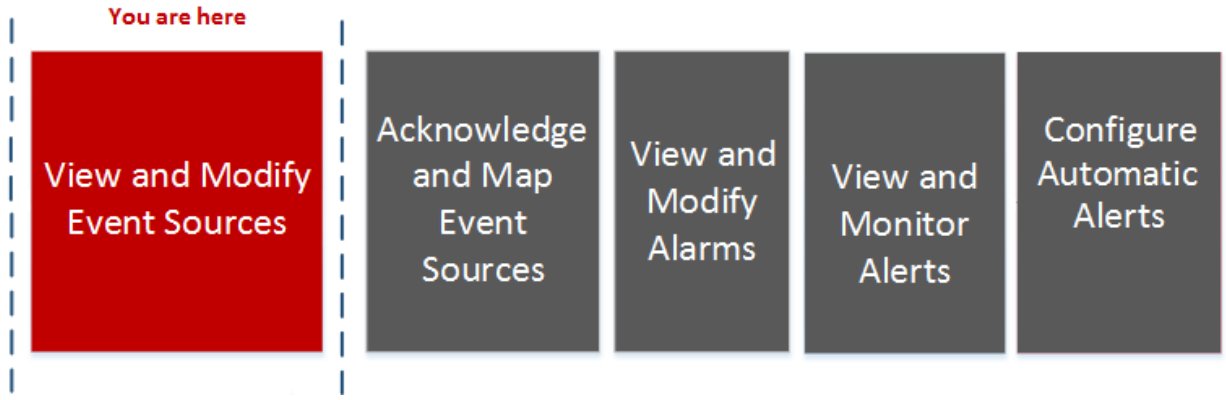
Ansicht „Ereignisquellen“

Der Bereich „Ereignisquellenattribute“ hat folgende Registerkarten.

Um auf diesen Bereich zuzugreifen, navigieren Sie zu **ADMIN > Ereignisquellen**.

Workflow

Dieser Workflow zeigt das End-to-End-Verfahren zum Ändern, Bestätigen, Zuordnen und Konfigurieren von Ereignisquellen, zusammen mit der Anzeige und Konfiguration von Ereignisquellenalarmen und zugehörigen Warnmeldungen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Ereignisquellengruppe erstellen	Erstellen von Ereignisquellengruppen
Administrator	Ereignisquellengruppe bearbeiten oder löschen	Bearbeiten oder Löschen von Ereignisquellengruppen
Administrator	Ereignisquellenattribute bearbeiten	Erstellen von Ereignisquellen und Bearbeiten von Attributen

Verwandte Themen

Managen von Ereignisquellengruppen

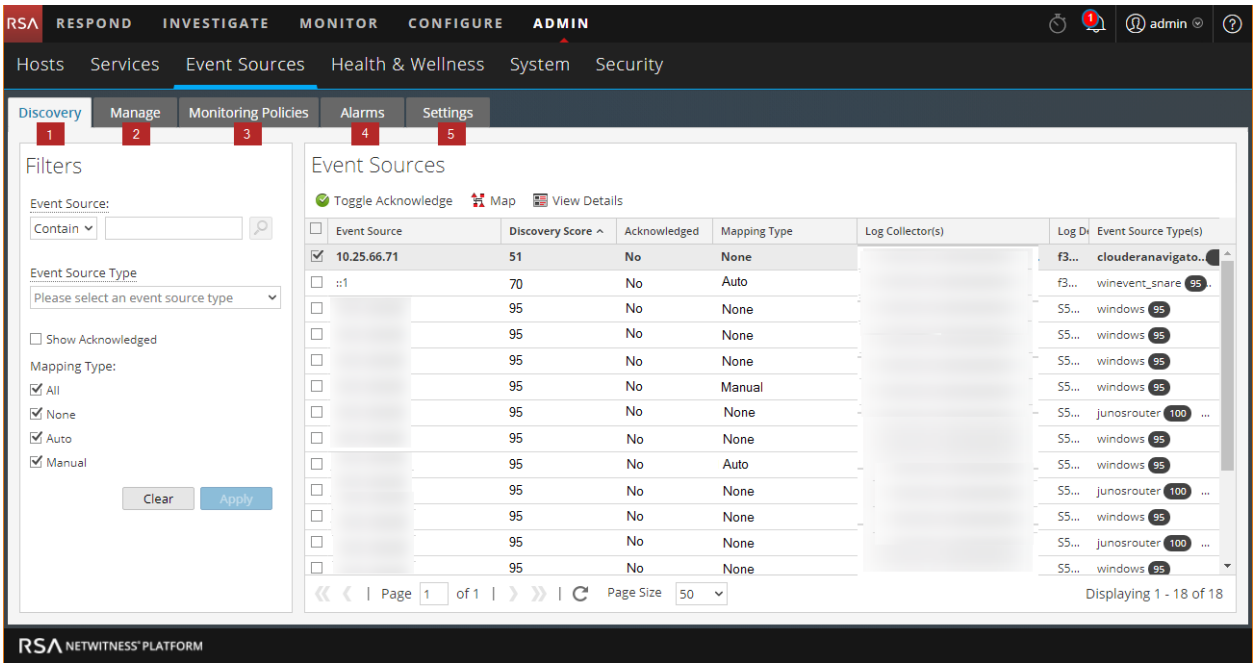
Erstellen von Ereignisquellengruppen

Bearbeiten oder Löschen von Ereignisquellengruppen

Erstellen von Ereignisquellen und Bearbeiten von Attributen

Überblick

Die Ansicht „Ereignisquellen“ enthält die Details für Ereignisquellen, die von RSA NetWitness® Platform erkannt, bestätigt oder zugeordnet werden.



1 Registerkarte „Erkennung“

Verwenden Sie diese Registerkarte, um die Ereignisquellentypen einzusehen, die NetWitness für jede Adresse ermittelt hat, und die Zuverlässigkeit des Systems hinsichtlich der Wahrscheinlichkeit, dass sie korrekt identifiziert wurden.

2 Registerkarte „Managen“

Verwenden Sie diese Registerkarte, um Ereignisquellengruppen zu erstellen, zu bearbeiten und zu löschen. Sie präsentiert eine anpassbare, durchsuchbare Ansicht all Ihrer Ereignisquellen und Gruppen.

3 Registerkarte Überwachungsrichtlinien

Verwenden Sie diese Registerkarte, um die Warnmeldungskonfiguration für Ereignisquellen zu managen.

4 Registerkarte „Alarme“

Verwenden Sie diese Registerkarte, um die Details der Alarme anzuzeigen, die erzeugt wurden.

5 Registerkarte „Einstellungen“

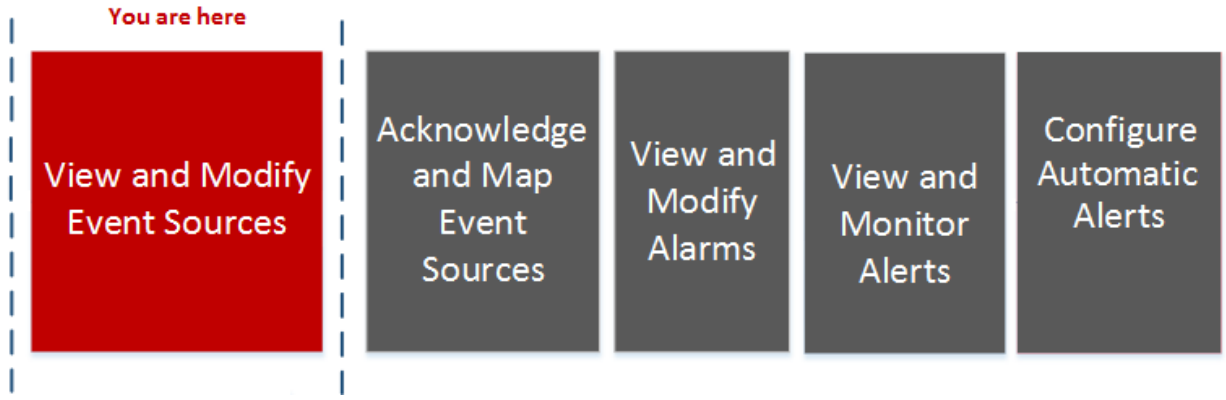
Verwenden Sie diese Registerkarte, um das Verhalten für automatische (Baseline-) Warnmeldungen anzuzeigen oder zu ändern.

Erstellen/Bearbeiten von Gruppenformularen

Dieses Formular „Ereignisquellengruppe erstellen“ wird angezeigt, wenn Sie eine Ereignisquellengruppe erstellen oder bearbeiten.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	* Anzeigen und Ändern von Ereignisquellen.	Managen von Ereignisquellengruppen
Administrator	Bestätigen und Zuordnen von Ereignisquellen.	Bestätigen und Zuordnen von Ereignisquellen
Administrator	Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.	Parser-Zuordnungen verwalten
Administrator	Anzeigen von Ereignisquellenalarmen.	Anzeigen von Ereignisquellenalarmen
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

Formular zum Erstellen von Ereignisquellengruppen

Managen von Ereignisquellengruppen

Detailansicht

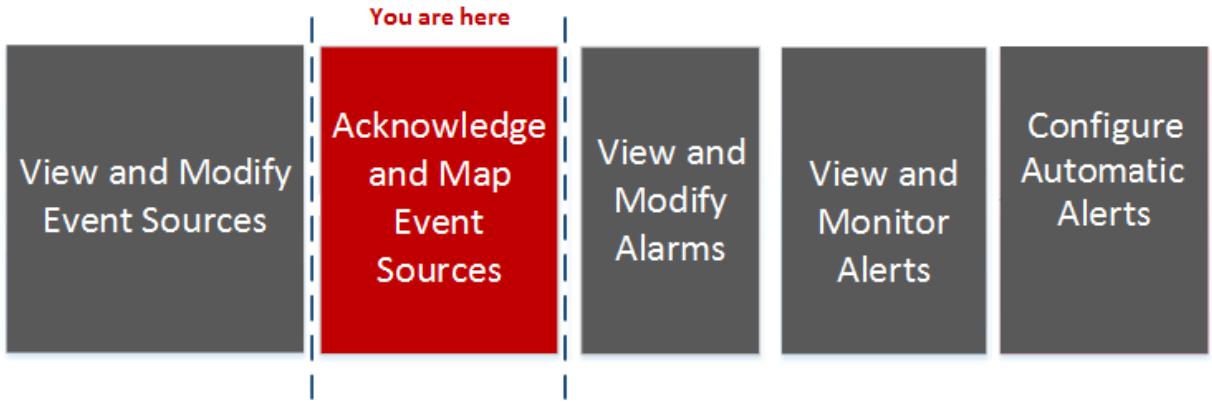
In der **Detailansicht** finden Sie Details zu der betreffenden Ereignisquellen sowie einen Auszug aus den für die verschiedenen Typen erkannten Protokolle. So können Sie die Korrektheit beurteilen.

Der Zugriff auf die **Detailansicht** ist auf mehrere Arten möglich:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Details anzeigen**. Alternativ:
- Doppelklicken Sie auf die Ereignisquelle, die Sie ausgewählt haben.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Anzeigen und Ändern von Ereignisquellen.	Managen von Ereignisquellengruppen
Administrator	*Bestätigen und zuordnen von Ereignisquellen.	Bestätigen und Zuordnen von Ereignisquellen
Administrator	Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.	Parser-Zuordnungen verwalten
Administrator	Anzeigen von Details zum Protokollparser	Parser-Zuordnungen verwalten
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

*Sie können diese Aufgabe hier durchführen.

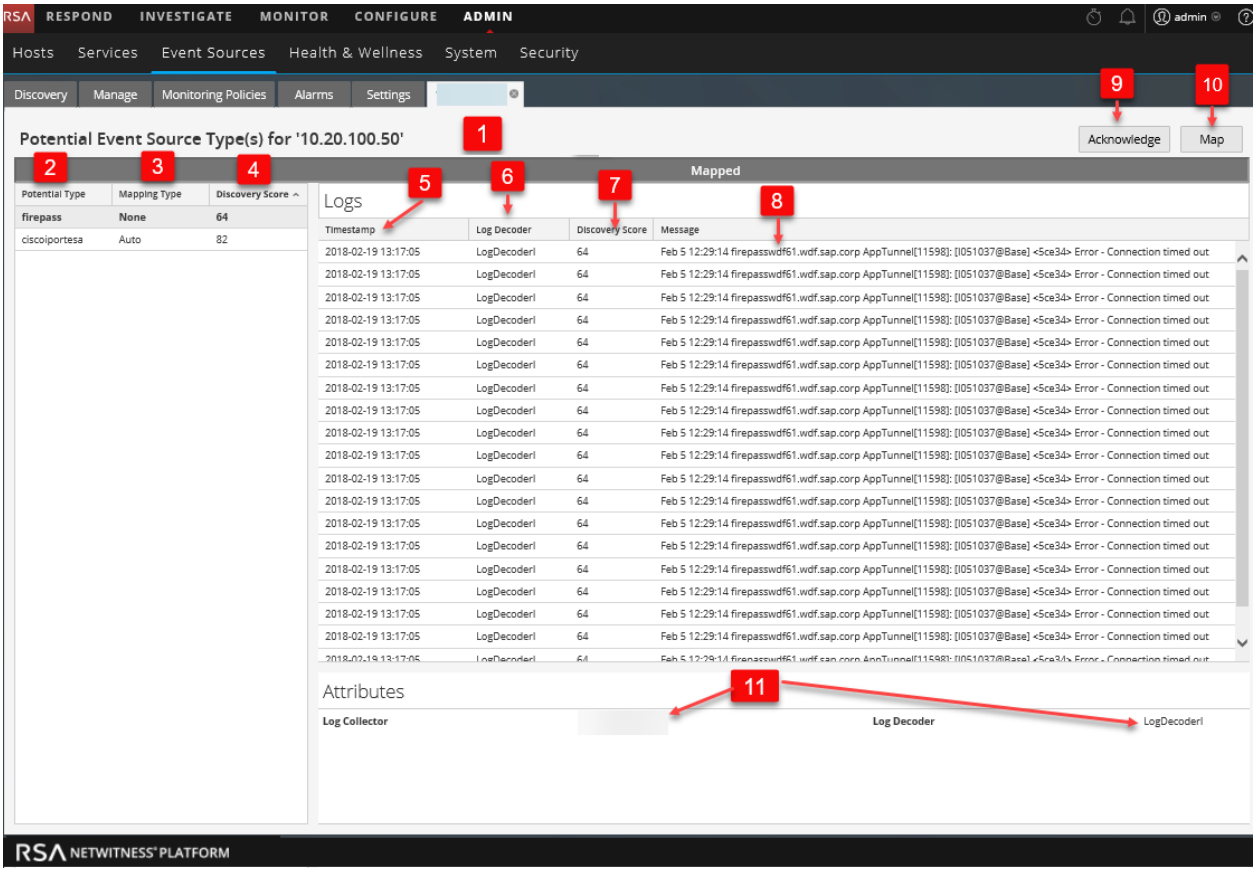
Verwandte Themen

Anzeigen von Protokollen von einer Log Decoder-Version vor 11.0

Überblick

Das folgende Beispiel zeigt die Discovery Scores, Ereignisquellentypen, Protokolle und Attribute für die Ereignisquelle, die Sie im Bereich „Ereignisquellen“ ausgewählt haben, für einen einzigen Log Decoder.

Hinweis: Geräteprotokolle sind nur für Log Decoder in der Version 11.0.0.0 und neuere Versionen verfügbar.



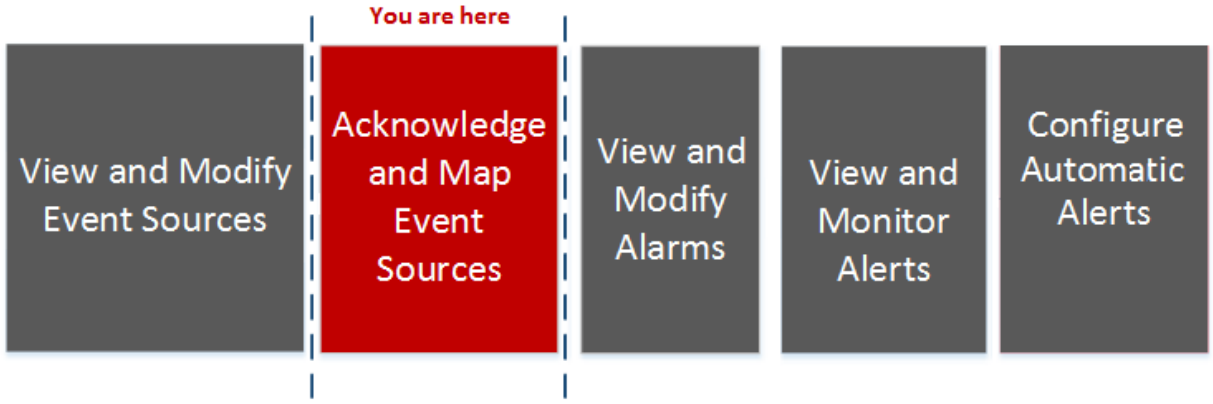
1	Zeigt die Adresse der ausgewählten Ereignisquelle an.
2	Zeigt den potenziellen Typ der ausgewählten Ereignisquelle an.
3	Zeigt den ausgewählten Typ der Ereignisquellenzuordnung als „Automatisch zugeordnet“, „Manuell zugeordnet“ oder „Ohne“ an. Änderungen an der Ereignisquellenzuordnung werden nur hier angezeigt.
4	Zeigt den Erkennungswert des ausgewählten Ereignisquellentyps an (0 = niedrigste Zuverlässigkeit, 100 = höchste Zuverlässigkeit).
5	Zeigt die Zeitstempel der letzten Protokolle an, die für den ausgewählten Ereignisquellentyp analysiert wurden
6	Zeigt die Adresse des Log Decoders an, der Ereignisquellen analysiert
7	Zeigt den Discovery Score des zugehörigen Protokolls an
8	Zeigt die Protokolle für den ausgewählten Ereignisquellentyp an
9	Ermöglicht die Bestätigung, dass alle erkannten Ereignisquellentypen korrekt sind
10	Ermöglicht die Einstellungen der passenden Parser für die ausgewählten Ereignisquellenadressen
11	Zeigt die zur Ereignisquellenmanagement verwendeten Attribute des ausgewählten Ereignisquellentyps an

Parser-Zuordnungen verwalten

Im Dialogfeld **Parser-Zuordnungen verwalten** können Sie ausgewählten Ereignisquellenadressen passende Parser zuordnen. Klicken Sie in der **Detailansicht** auf die Schaltfläche **Zuordnen**.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen.



Was möchten Sie tun?

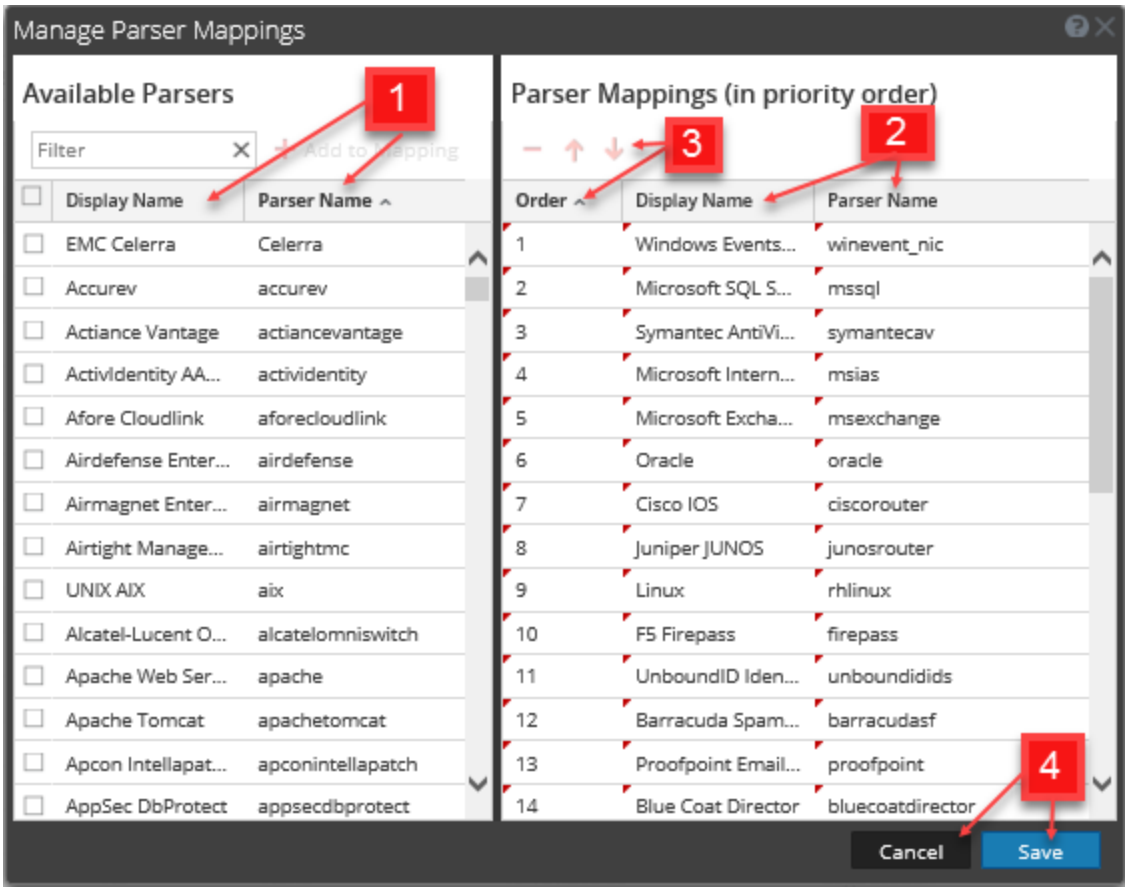
Rolle	Ziel	Dokumentation
Administrator	Anzeigen und Ändern von Ereignisquellen.	Managen von Ereignisquellengruppen
Administrator	Bestätigen und Zuordnen von Ereignisquellen.	Bestätigen und Zuordnen von Ereignisquellen
Administrator	* Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.	Parser-Zuordnungen verwalten
Administrator	Anzeigen von Ereignisquellenalarmen.	Anzeigen von Ereignisquellenalarmen
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

Anzeigen von Protokollen von einer Log Decoder-Version vor 11.0

Überblick



1	Zeigt alle zum Zuordnen verfügbaren Parser an, basierend auf den Ereignisquellen, die Sie in der Ansicht **Erkennung** ausgewählt haben. Zeigt außerdem die Zuordnungen an, die bereits in den Log Decodern für die ausgewählte Ereignisquelle vorhanden sind, oder alle erkannten Parser. Wenn Sie die verfügbaren Parser filtern möchten: Geben Sie die ersten Buchstaben des Namens des Parsers ein, den Sie zuordnen möchten. Klicken Sie auf die Schaltfläche **Zu Zuordnung hinzufügen**, um den Parser den im rechten Bereich aufgeführten Parserzuordnungen hinzuzufügen. Die Schaltfläche **Zu Zuordnung hinzufügen** wird erst aktiviert, wenn Sie Parser auswählen. Klicken Sie auf die Schaltfläche **Zu Zuordnung hinzufügen** im rechten Bereich, um den jeweils ausgewählten Parser hinzuzufügen. Mithilfe der Nach-oben-Taste und der Nach-unten-Taste können Sie die Reihenfolge der Parserzuordnungen anpassen. Zudem können Sie ausgewählten Parserzuordnungen per Drag-and-Drop verschieben. Durch Drücken der **STRG**-Taste lassen sich mehrere Zuordnungen auswählen.
2	Zeigt die Namen der ausgewählten Parser an, die zugeordnet werden sollen.
3	Zeigt die Reihenfolge der ausgewählten Parserzuordnungen an. Durch Klicken auf das Minus-Symbol ( ) können Sie Parserzuordnungen löschen. Drücken Sie die Taste **STRG**, um mehrere Zuordnungen auszuwählen und Gruppenvorgänge auf sie anzuwenden.

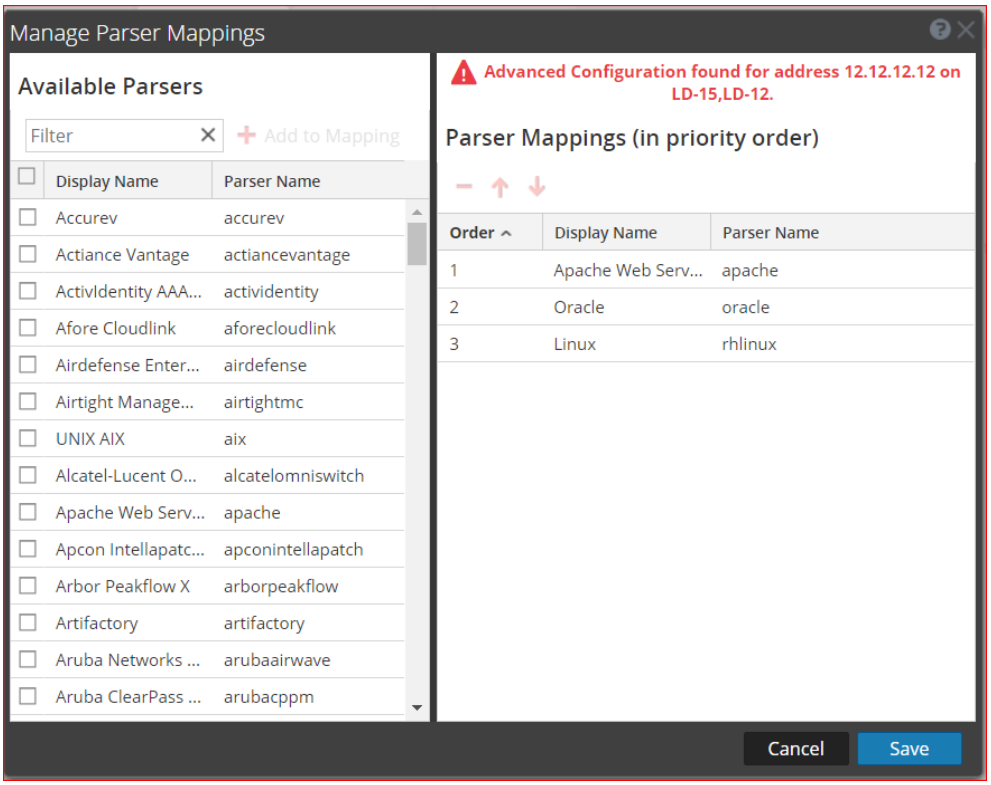
4 Klicken Sie auf **Speichern**, um die Zuordnungen in allen Log Decodern zu speichern. Eine Pop-up-Meldung informiert Sie, dass Ihre Zuordnungen erfolgreich gespeichert wurden. Sobald Sie das Fenster schließen, wird das Banner auf der Registerkarte **Details** mit dem neuen Status aktualisiert. Falls eine Zuordnung vorhanden ist, wird der Text **Zugeordnet** angezeigt.
Klicken Sie auf **Abbrechen**, um zur Registerkarte **Details** zurückzukehren.

Erweiterte Konfiguration

Mit Log Collector vorgenommene Zuordnungskonfigurationen werden nicht im Fenster „Parser-Zuordnungen“ angezeigt. Wenn die Zuordnung gespeichert wird, wird sie für die entsprechende IP-Adresse gespeichert, nicht für den entsprechenden Log Collector-Eintrag. Wenn keine Zuordnungen für die betreffende IP-Adresse gefunden werden, werden die erkannten Ereignisquellentypen im Fenster „Parser-Zuordnungen“ angezeigt.

Werden erweiterte Log Decoder-Konfigurationen erkannt, wird eine Meldung ähnlich der folgenden im Dialogfeld „Parser-Zuordnungen verwalten“ angezeigt.

Hinweis: Wenn Sie die erweiterte Konfiguration bearbeiten möchten, müssen Sie im Log Decoder-Service zu den Konfigurationsoptionen für Parser-Zuordnungen navigieren.



Registerkarte „Alarme“

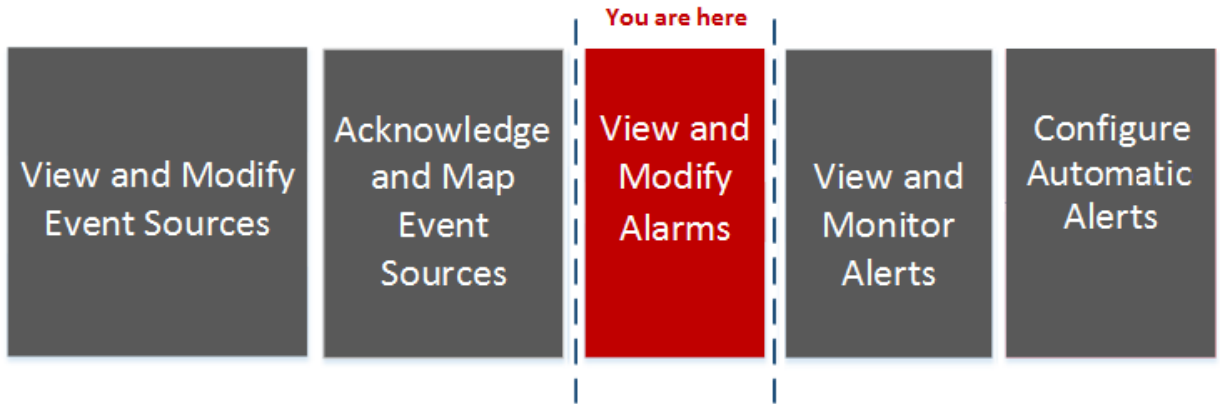
Auf der Registerkarte „Alarme“ finden Sie Details zu allen erzeugten Alarmen.

Die Registerkarte „Alarme“ besteht aus einem einzigen Bereich, in dem der Status der Alarme angezeigt wird.

Öffnen können Sie diese Registerkarte durch Klicken auf ADMIN > „Ereignisquellen“ > „Alarme“.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen. Er zeigt auch, an welcher Stelle im Prozess die Konfiguration von Alarmen und Warnmeldungseinstellungen angeordnet ist.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Anzeigen und Ändern von Ereignisquellen.	Managen von Ereignisquellengruppen
Administrator	Bestätigen und Zuordnen von Ereignisquellen.	Bestätigen und Zuordnen von Ereignisquellen
Administrator	Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.	Parser-Zuordnungen verwalten
Administrator	* Anzeigen von Ereignisquellenalarmen.	Anzeigen von Ereignisquellenalarmen
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

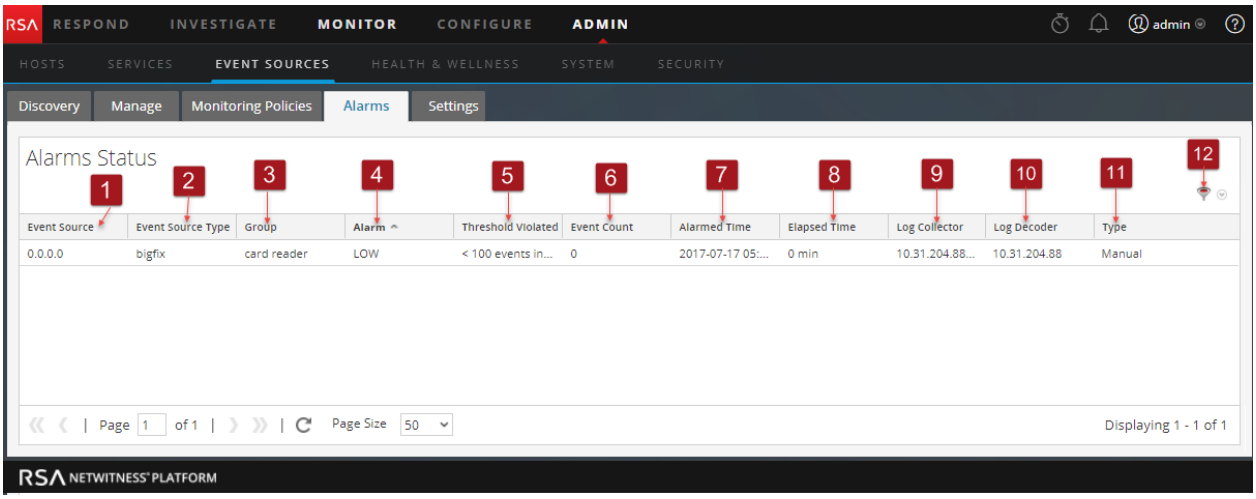
*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

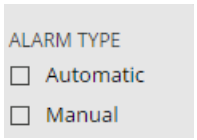
[Konfigurieren von automatischen Warnmeldungen]

Überblick

Die Registerkarte „Alarme“ enthält die Details für Ereignisquellen, die derzeit gegen eine Policy verstoßen oder Schwellenwerte über- oder unterschreiten. Nur Ereignisquellen, die gegen eine Policy verstoßen, werden in der Liste angezeigt. Wenn die Ereignisquelle in einen normalen Zustand zurückkehrt, wird der entsprechende Alarm in der Liste nicht mehr angezeigt



1	Zeigt die IP-Adresse, die IPv6-Adresse oder den Hostnamen der alarmierten Ereignisquelle an.
2	Zeigt den Typ der alarmierten Ereignisquelle an. Beispiel: **winevent_nic** (für Microsoft Windows) oder **rhlinux** (für Linux).
3	Zeigt die Ereignisquellengruppe an, zu der die Ereignisquelle gehört, für die der Alarm ausgelöst wurde.
4	Zeigt den Typ des Schwellenwerts an, der ausgelöst wurde: **Hoch** oder **Niedrig**
5	Zeigt die Bedingungen des Schwellenwerts an, der ausgelöst wurde. Beispiel: `5,000,000 events in 5 minutes`
6	Zeigt an, wie viele Ereignisse in dem Schwellenwertzeitraum erfasst wurden, der den Alarm ausgelöst hat.
7	Zeigt an, wann die Ereignisquelle erstmals alarmiert wurde. **Hinweis:** Wenn Sie erstmals auf diese Ansicht zugreifen, sind die Daten nach dieser Spalte sortiert (neuester Alarm zuerst).
8	Zeigt an, wie viel Zeit seit der Alarmierung der Ereignisquelle verstrichen ist.
9	Zeigt den Log Collector an, der zuletzt Daten von dieser Ereignisquelle erfasst hat.
10	Zeigt den Log Decoder an, der zuletzt Daten von dieser Ereignisquelle empfangen hat.
11	Zeigt den Typ des Alarms an. Typ des Alarms ist entweder **Manuell** oder **Automatisch**: • **Manuell**: Dies sind Alarme, die die konfigurierte Schwellenwertrichtlinie verletzen. • **Automatisch**: Dies sind Alarme, die für die alarmierte Ereignisquelle von der Baseline abweichen
12	Klicken Sie auf das **Filter**-Symbol, um das **Filtern**-Menü anzuzeigen:



Wählen Sie entweder **Automatisch** oder **Manuell** aus:

- Wenn Sie **Automatisch** auswählen, werden nur die Warnmeldungen angezeigt, die auf Baselines basieren.
- Wenn Sie **Manuell** auswählen, werden nur die Alarme angezeigt, für die Sie Schwellenwerte festgelegt haben.

Hinweis: Sie können Spalten ausblenden oder anzeigen, indem Sie mit der rechten Maustaste in die Tabellenkopfzeile klicken und **Spalten** aus dem Drop-down-Menü auswählen. Wählen Sie eine Spalte aus, um sie anzuzeigen, oder deaktivieren Sie die Spalte, um sie auszublenden.

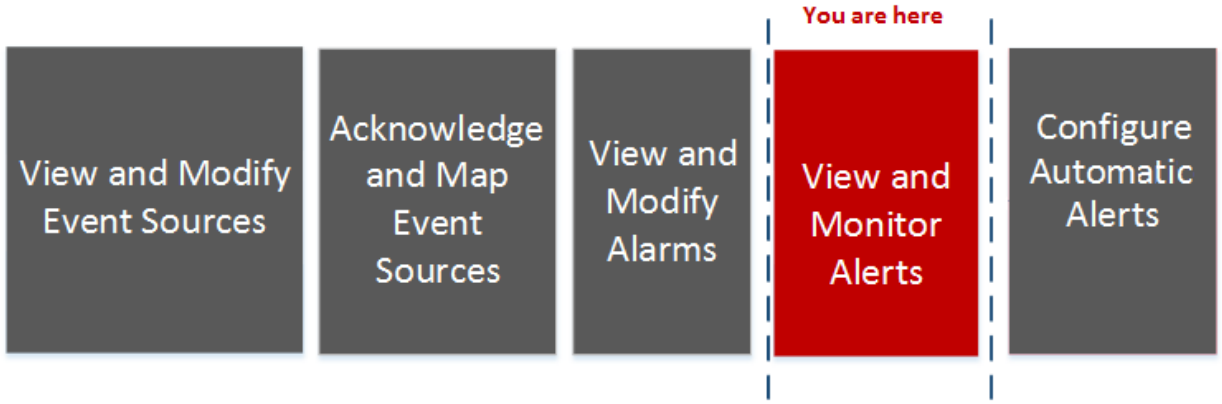
Registerkarte Überwachungsrichtlinien

Auf der Registerkarte „Überwachungsrichtlinien“ sind die Schwellenwerte nach Ereignisquellengruppe sortiert.

Klicken Sie zum Öffnen der Registerkarte auf **ADMIN > Ereignisquellen**. Die Registerkarte **Managen** wird angezeigt. Wählen Sie die Registerkarte **Überwachungsrichtlinien** aus.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Anzeigen und Ändern von Ereignisquellen.	Managen von Ereignisquellengruppen
Administrator	Bestätigen und Zuordnen von Ereignisquellen.	Bestätigen und Zuordnen von Ereignisquellen
Administrator	Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.	Parser-Zuordnungen verwalten
Administrator	Anzeigen von Ereignisquellenalarmen.	Anzeigen von Ereignisquellenalarmen
Administrator	* Anzeigen von Überwachungsrichtlinien.	Überwachungsrichtlinien
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

Einrichten von Benachrichtigungen

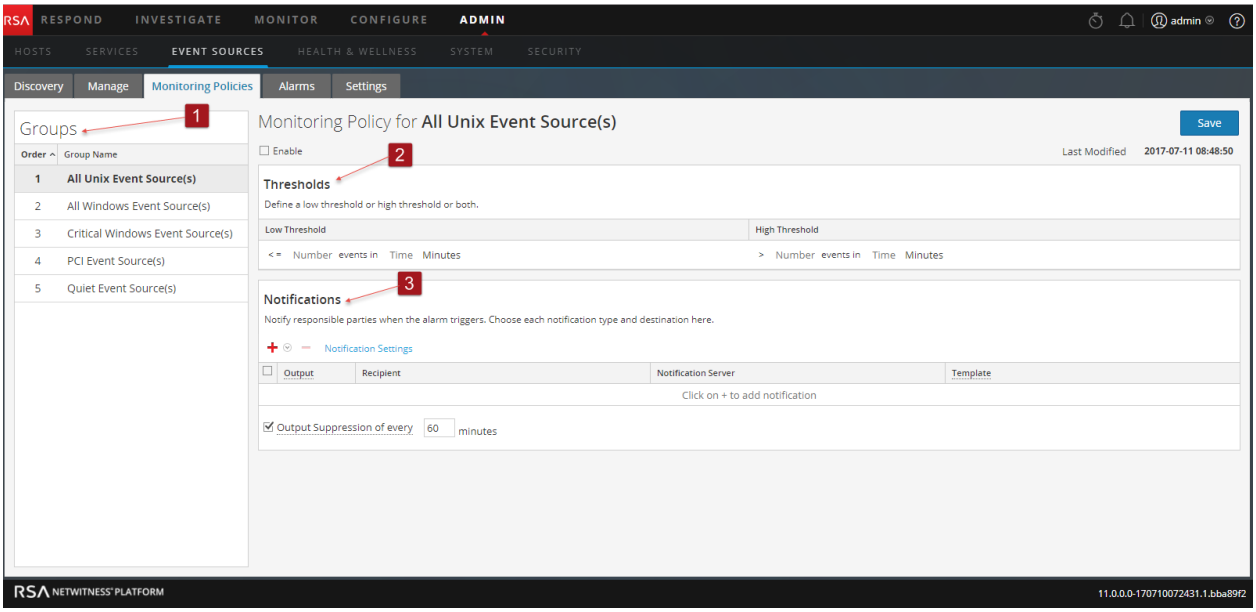
Deaktivieren von Benachrichtigungen

Überblick

Die Registerkarte **Überwachungsrichtlinien** umfasst drei Bereiche.

- Bereich mit Ereignisgruppen
- Bereich „Schwellenwerte“
- Bereich „Benachrichtigungen“

Die Abbildung unten zeigt ein Beispiel für die Registerkarte **Überwachungsrichtlinien**.



1 Bereich „Gruppen“
2 Bereich „Schwellenwerte“
3 Bereich „Benachrichtigungen“

Bereich mit Ereignisgruppen

Mit der Auswahl einer Gruppe in diesem Bereich legen Sie fest, welche Schwellenwerte im Bereich „Schwellenwerte“ angezeigt werden sollen. Für jede Ereignisquellengruppe kann ein eigener Satz Schwellenwerte festgelegt werden. Beachten Sie, dass die Gruppen in einer bestimmten Reihenfolge angeordnet sind:

- Per Drag-and-drop können Sie Gruppen in die gewünschte Reihenfolge ziehen.
- Je höher eine Gruppe in der Liste steht, desto höher ist der Rang der Schwellenwerte dieser Gruppe: RSA NetWitness Platform prüft die Schwellenwerte in der Reihenfolge, die in diesem Bereich festgelegt ist. Daher sollten Sie Gruppen mit höchster Priorität ganz oben in der Liste einordnen

Bereich Schwellenwerte

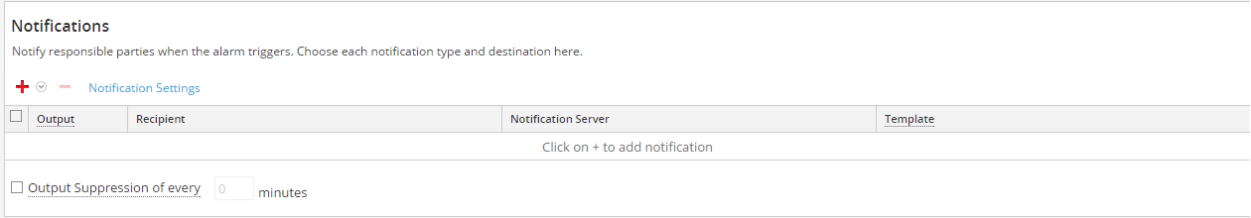
Die Abbildung unten zeigt ein Beispiel für den Bereich „Schwellenwerte“ einer Ereignisquellengruppe.

Der Bereich „Schwellenwerte“ enthält die nachfolgend aufgeführten Funktionen.

Funktion	Beschreibung
Aktivieren	Über das Kontrollkästchen „Aktivieren“ legen Sie fest, ob die für eine Gruppe definierten Schwellenwerte aktiviert sind. Falls aktiviert, werden immer dann, wenn die Schwellenwerte dieser Gruppe einen Wert außerhalb des definierten Bereichs erreichen, Benachrichtigungen versandt. Falls sie nicht aktiviert sind, findet keine Überwachung der betreffenden Ereignisquellengruppe statt. **Hinweis:** Wenn Sie einen Schwellenwert konfigurieren und versuchen, die Seite zu speichern, ohne ihn zu aktivieren, werden Sie in einer Bestätigungsmeldung gefragt, ob die Policy aktiviert werden soll oder nicht. Wenn Sie eine Policy aktivieren, aber keine Schwellenwerte festgelegt haben, können Sie dennoch automatische (Baseline-) Benachrichtigungen erhalten, sofern Sie automatische Benachrichtigungen aktiviert haben. Nachstehend finden Sie weitere Informationen zur Anzeige von Benachrichtigungen.
Niedrige Anzahl der Ereignisse Niedrige Anzahl der Minuten bzw. Stunden	Dies ist der untere Bereich des Schwellenwerts. Geben Sie die Untergrenzen für die Anzahl der Ereignisse und den Zeitbereich an. Wenn die Ereignisquellengruppe weniger Meldungen als hier angegeben erhält, wird der Schwellenwert nicht erreicht, woraufhin Benachrichtigungen versandt werden.
Hohe Anzahl der Ereignisse Hohe Anzahl der Minuten oder Stunden	Funktioniert ähnlich wie für die niedrigen Werte: Wenn mehr Meldungen als hier angegeben eingehen, wird der Schwellenwert verfehlt, woraufhin Benachrichtigungen versandt werden.
Datum und Uhrzeit der letzten Änderung	Das Feld enthält Datum und Uhrzeit der letzten Änderung der Schwellenwerte.
Speichern	Speichert die an den Schwellenwerten vorgenommenen Änderungen.

Bereich Benachrichtigungen

Die Abbildung unten zeigt ein Beispiel für den Bereich „Benachrichtigungen“ einer Ereignisquellengruppe.

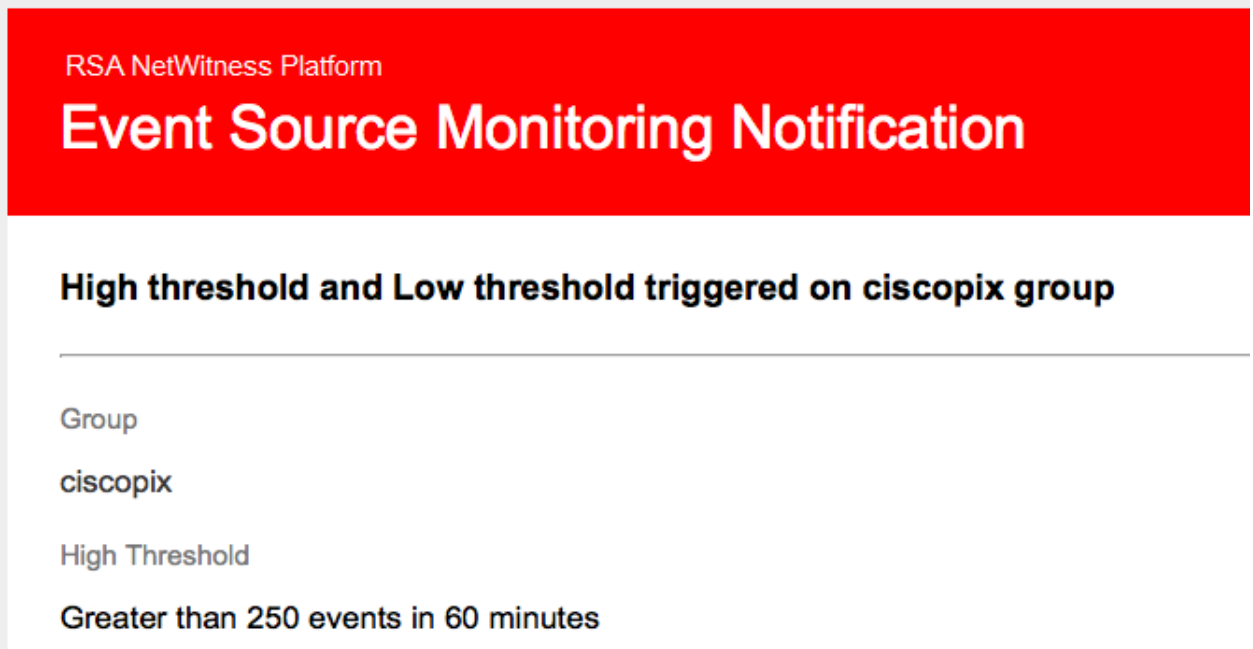


In der folgenden Tabelle werden die Felder im Bereich Benachrichtigungen beschrieben.

Feld	Beschreibung
Tools + -	Folgende Optionen sind in der Symbolleiste verfügbar: • **Hinzufügen (+)**: durch Klicken auf **Hinzufügen** wird ein Menü angezeigt, in dem Sie den Benachrichtigungstyp auswählen können • **Entfernen (-)**: Entfernt die ausgewählte Zeile aus der Liste.
Benachrichtigungseinstellungen	Durch Klicken auf diesen Link wird die Seite **Admin** > **System** > **Benachrichtigungen** in NetWitness Platform in einer neuen Browserregisterkarte geöffnet.
Typ	Zeigt den Typ der ausgewählten Benachrichtigung an. Folgende Optionen stehen zur Verfügung: • E-Mail • SNMP • Syslog
Benachrichtigung	Weitere Informationen finden Sie unter **Konfigurieren von Benachrichtigungsausgaben** im *Systemkonfigurationsleitfaden*.
Benachrichtigungsserver	Weitere Informationen finden Sie unter **Konfigurieren von Benachrichtigungsservern** im *Systemkonfigurationsleitfaden*
Vorlage	RSA hält für das Ereignisquellenmanagement drei Standardvorlagen für Benachrichtigungen bereit. Sie können entweder die vorliegenden Vorlagen verwenden oder sie entsprechend den Anforderungen Ihrer Organisation anpassen: • **E-Mail-Vorlage**: sendet Benachrichtigungen an die angegebenen E-Mail-Adressen. • **SNMP-Vorlage**: sendet Benachrichtigungen an den angegebenen SNMP-Server. • **Syslog-Vorlage**: sendet Benachrichtigungen an den angegebenen Syslog-Server. Weitere Informationen finden Sie unter **Konfigurieren von Vorlagen für Benachrichtigungen** im *Systemkonfigurationsleitfaden*.

Feld	Beschreibung
Ausgabeunterdrückung	Mithilfe dieses Elements kann die Anzahl von Benachrichtigungen für diese Richtlinie begrenzt werden, falls es in einem kurzen Zeitraum zu sehr vielen Alarmmeldungen kommt.

Nachstehend sind Beispiele für Benachrichtigungen aufgeführt, die auf den bereitgestellten Vorlagen basieren:



- E-Mail:

  Für E-Mail-Benachrichtigungen gibt die dritte Spalte, **Alarmtyp**, an, ob der ausgelöste Alarm auf einem Nutzerschwellenwert basiert oder ob die Baselinedaten außerhalb ihrer normalen Grenzen liegen. Wenn die automatische Überwachung oder Benachrichtigungen deaktiviert sind, erhalten Sie keine automatischen Benachrichtigungen. Dasselbe gilt für Syslog und SNMP, außer dass jene Benachrichtigungen anders formatiert sind.

- SNMP-Trap:

```
11-11-2015 11:57:33 Local7.Debug 127.0.0.1 community=public,
enterprise=1.3.6.1.4.1.36807.1.20.1, uptime=104313, agent_
ip=10.251.37.92, version=Ver2, 1.3.6.1.4.1.36807.1.20.1="NetWitness
Platform Event Source Monitoring Notification:
Group: PCI Event Source(s)
High Threshold:
Greater than 500 events in 5 minutes
10.17.0.10,ciscopix,Manual
10.17.0.13,ciscopix,Manual
10.17.0.8,ciscopix,Manual
10.17.0.8,ciscopix,Automatic
```

```
10.17.0.12,ciscopix,Manual
10.17.0.5,ciscopix,Manual
10.17.0.6,ciscopix,Manual
10.17.0.4,ciscopix,Manual
10.17.0.4,ciscopix,Automatic
10.17.0.3,ciscopix,Manual"
```

- Syslog-Beispiel:

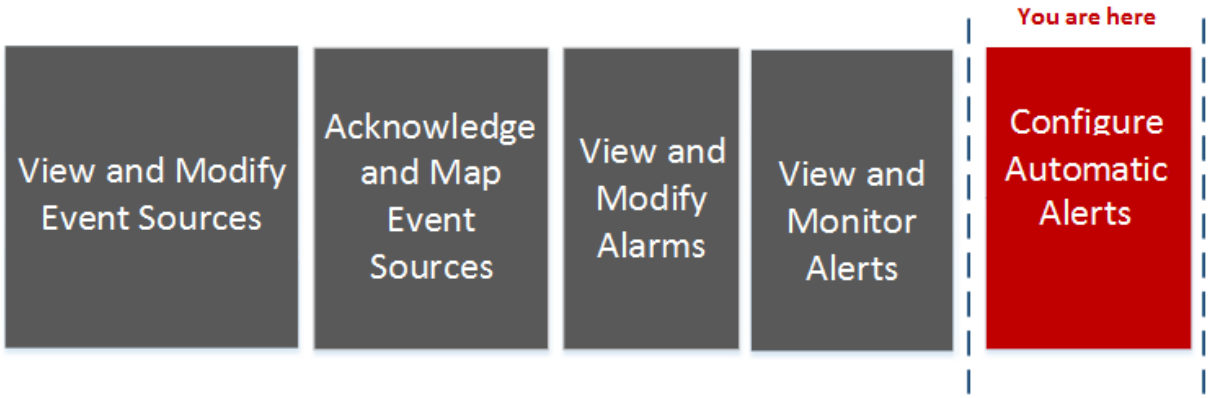
```
11-11-2015 11:57:33 User.Info 127.0.0.1 Nov 11 11:57:33 localhost
CEF:0|RSA|NetWitness Platform Event Source Monitoring|10.6.0.0.0|
HighThresholdAlert|ThresholdExceeded|1|cat=PCI Event Source(s)|Devices|
src=10.17.0.10,ciscopix,Manual|src=10.17.0.13,ciscopix,Manual|src=10.1
7.0.8,ciscopix,Manual|src=10.17.0.8,ciscopix,Automatic|src=10.17.0.12,
ciscopix,Manual|src=10.17.0.5,ciscopix,Manual|src=10.17.0.6,ciscopix,M
anual|src=10.17.0.4,ciscopix,Manual|src=10.17.0.4,ciscopix,Automatic|s
rc=10.17.0.3,ciscopix,Manual|
```

Registerkarte „Einstellungen“

Die Registerkarte „Einstellungen“ enthält Optionen zur automatischen Überwachung (Baseline-Warnmeldungen). Um auf diese Registerkarte zuzugreifen, navigieren Sie zu ADMIN > Ereignisquellen > Einstellungen.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess zur Konfiguration von Ereignisquellen.



Was möchten Sie tun?

Rolle	Ziel	Dokumentation
Administrator	Anzeigen und Ändern von Ereignisquellen.	Managen von Ereignisquellengruppen
Administrator	Bestätigen und Zuordnen von Ereignisquellen.	Bestätigen und Zuordnen von Ereignisquellen
Administrator	Hinzufügen und Konfigurieren von Parser-Zuordnungen für einen Log Decoder.	Parser-Zuordnungen verwalten
Administrator	Anzeigen von Ereignisquellenalarmen.	Anzeigen von Ereignisquellenalarmen
Administrator	* Konfigurieren von automatischen Warnmeldungen.	Automatische Warnmeldungen
Administrator	Troubleshooting für das Ereignisquellenmanagement.	ESM-Troubleshooting & Anhang

*Sie können diese Aufgabe hier durchführen.

Verwandte Themen

Automatische Warnmeldungen

Deaktivieren von Benachrichtigungen

Überblick

Für Ereignisquellengruppen lassen sich Policies und Schwellenwerte festlegen. Sobald die Schwellenwerte nicht eingehalten werden, erhalten Sie eine Benachrichtigung. Darüber hinaus bietet NetWitness Platform auch die Möglichkeit für den automatisierten Versand von Alarmen, falls Sie keine Schwellenwerte zur Alarmerzeugung festlegen möchten.

Informationen über automatische Warnmeldungen

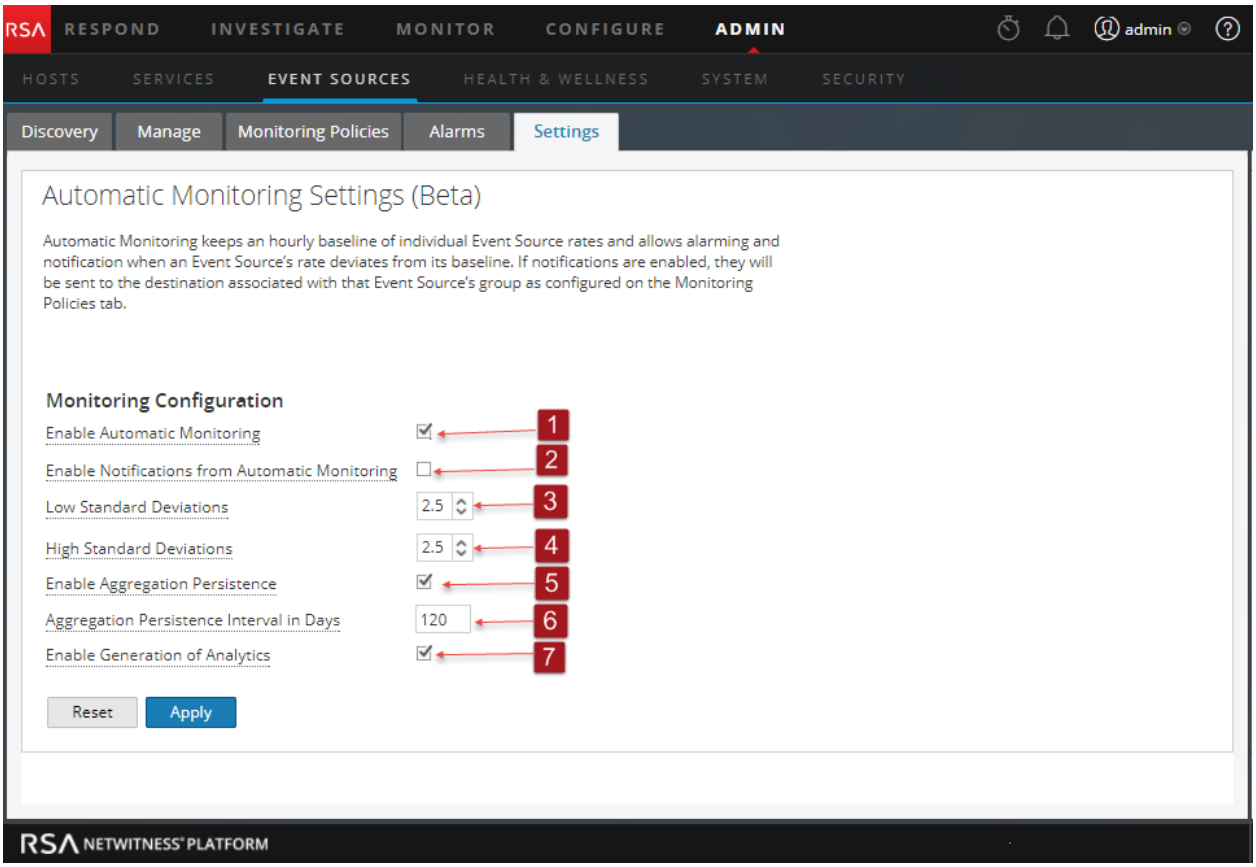
Sie können Policies und Schwellenwerte für Ihre Ereignisquellengruppen einrichten. So erhalten Sie Benachrichtigungen, wenn die Schwellenwerte nicht eingehalten werden. NetWitness Platform bietet darüber hinaus eine Methode, Alarme automatisch zu erhalten, wenn Sie keine Schwellenwerte einrichten möchten, um Alarme zu erzeugen.

Um automatische Warnmeldungen auszulösen, können Sie Baselinewerte verwenden. Auf diese Weisemüssen Sie nicht zahlreiche Gruppenschwellenwerte und -Policies einrichten, um Warnmeldungen zu erhalten. Jede ungewöhnliche Menge von Nachrichten löst Warnmeldungen aus, ohne dass eine Konfiguration erforderlich ist (außer dem Einschalten der automatischen Warnmeldungen).

Beachten Sie Folgendes:

- Sobald Sie damit beginnen, Nachrichten aus einer Ereignisquelle zu sammeln, braucht das System etwa eine Woche, um einen Baselinewert für diese Ereignisquelle zu speichern. Nach diesem ersten Zeitraum warnt Sie das System, wenn die Anzahl der Nachrichten für einen Zeitraum um eine bestimmte Menge über oder unter der Baseline liegen. Standardmäßig ist diese Menge 2 Standardabweichungen über oder unter der Baseline.
- Legen Sie Ihre Einstellungen der oberen und unteren Abweichung danach fest, wie „regelmäßig“ Ihre Ereignisquellen sich verhalten. D. h., wenn Sie keine oder nur wenig Abweichung in der Anzahl der Nachrichten erwarten, die in einem bestimmten Zeitraum eingehen (z. B. 8 bis 9 Uhr an einem Wochentag), können Sie einen niedrigen Wert für die Abweichung festlegen. Wenn Sie andererseits oft sehr hohe Abweichungen sehen, legen Sie den Abweichungswert höher fest.
- Wenn Sie eine Policy aktivieren, aber keine Schwellenwerte festgelegt haben, können Sie dennoch automatische (Baseline-) Benachrichtigungen erhalten, sofern Sie automatische Warnmeldungen aktiviert haben.

Hinweis: Automatische Warnmeldungen und ihre Einstellungen befinden sich derzeit im Betatest.



1	Bestimmt, ob automatische Warnmeldungen aktiviert oder deaktiviert sind. Diese Option ist standardmäßig ausgewählt (automatische Warnmeldungen sind eingeschaltet)
2	Bestimmt, ob Benachrichtigungen für automatische Warnmeldungen aktiviert oder deaktiviert sind. Diese Option ist standardmäßig deaktiviert (automatische Benachrichtigungen werden nicht gesendet, wenn automatische Warnmeldungen ausgelöst werden)
3	Bei Unterschreitung dieser Standardabweichungen erhalten Sie Warnmeldungen. Der Standardwert ist **2.0** (Wahrscheinlichkeit von 95 %).
4	Bei Überschreitung dieser Standardabweichungen erhalten Sie Warnmeldungen. Der Standardwert ist **2.0** (Wahrscheinlichkeit von 95 %).
5	Bei Auswahl dieser Option wird die Anzahl der Ereignisquelle im Intervall von einer Stunde gespeichert. Die erfassten Daten werden verwendet, um die Baselinewerte für jede Ereignisquelle zu bilden. • **Aktiviert (Standard)**: Eine Anzahl pro Stunde und Ereignisquelle wird in der zugrunde liegenden Datenbank gespeichert. Dieser einstündigen Zählungen (oder Aggregationen) bilden die Verlaufsbasis zur Berechnung des normalen Bereichs für jede Ereignisquelle. • **Deaktiviert**: Wenn der SMS-Server neu gestartet wird, wird die Ereignisquellenüberwachung keine Verlaufsdaten aufweisen, anhand derer der normale Bereich berechnet werden kann. Der Nutzer wird dann warten müssen, bis genügend Daten (etwa die Daten einer Woche) erfasst worden sind, um eine neue Grundlage für jede Ereignisquelle zu bilden.
6	Kontrolliert, wie viele Verlaufsdaten (siehe **Aggregierungspersistenz aktivieren**) für jede Ereignisquelle aufbewahrt werden. Der Standardwert von 120 Tagen bedeutet, dass etwa 4 Monate Verlaufsdaten aufbewahrt und verwendet werden, wenn die Basis für jede

Ereignisquelle rekonstruiert wird.

7 Wenn aktiviert, werden Daten über das Verhalten der automatischen Warnmeldungen auf Festplatte gespeichert. Der Standardwert ist **aktiviert**.

Die aufbewahrten Daten umfassen den Baselinewert im Laufe der Zeit und den Warnmeldungsverlauf für jede Ereignisquelle. Beachten Sie jedoch, dass Ereignisquellenadresse und -typ anonymisiert sind. Es wird also nur Ihre Ereignisrate angezeigt.

Da automatische Warnmeldungen eine Betafunktion ist, sind diese Daten wichtig, um die Wirksamkeit der Funktion zu messen. Dies kann ohne Auswirkung auf die Funktion der automatischen Warnmeldungen deaktiviert werden.

8 Die Option **Zurücksetzen** verwirft alle ungespeicherten Änderungen für alle Einstellungen auf der Seite.

9 Klicken Sie auf **Anwenden**, um alle Änderungen an den Werten auf dieser Seite zu speichern.

Funktionen

Die Registerkarte „Einstellungen“ enthält die folgenden Funktionen.

Funktion	Beschreibung
Automatische Überwachung aktivieren	Bestimmt, ob automatische Warnmeldungen aktiviert oder deaktiviert sind. Diese Option ist standardmäßig ausgewählt (automatische Warnmeldungen sind eingeschaltet)
Benachrichtigungen von der automatischen Überwachung aktivieren	Bestimmt, ob Benachrichtigungen für automatische Warnmeldungen aktiviert oder deaktiviert sind. Diese Option ist standardmäßig deaktiviert (automatische Benachrichtigungen werden nicht gesendet, wenn automatische Warnmeldungen ausgelöst werden)
Untere Standardabweichungen	Bei Unterschreitung dieser Standardabweichungen erhalten Sie Warnmeldungen. Der Standardwert ist **2.0** (Wahrscheinlichkeit von 95 %).
Obere Standardabweichungen	Bei Überschreitung dieser Standardabweichungen erhalten Sie Warnmeldungen. Der Standardwert ist **2.0** (Wahrscheinlichkeit von 95 %).

Funktion	Beschreibung
Aggregierungspersistenz aktivieren	Bei Auswahl dieser Option wird die Anzahl der Ereignisquelle im Intervall von einer Stunde gespeichert. Die erfassten Daten werden verwendet, um die Baselinewerte für jede Ereignisquelle zu bilden. • Aktiviert (Standard): Eine Anzahl pro Stunde und Ereignisquelle wird in der zugrunde liegenden Datenbank gespeichert. Dieser einstündigen Zählungen (oder Aggregationen) bilden die Verlaufsbasis zur Berechnung des normalen Bereichs für jede Ereignisquelle. • Deaktiviert: Wenn der SMS-Server neu gestartet wird, wird die Ereignisquellenüberwachung keine Verlaufsdaten aufweisen, mit denen der normale Bereich berechnet werden kann, und der Nutzer wird warten müssen, bis genügend Daten (etwa die Daten einer Woche) erfasst werden, um eine neue Grundlage für jede Ereignisquelle zu bilden.
Intervall für Aggregierungspersistenz in Tagen	Kontrolliert, wie viele Verlaufsdaten (siehe **Aggregierungspersistenz aktivieren**) für jede Ereignisquelle aufbewahrt werden. Der Standardwert von 120 Tagen bedeutet, dass etwa 4 Monate Verlaufsdaten aufbewahrt und verwendet werden, wenn die Basis für jede Ereignisquelle rekonstruiert wird.
Erzeugung von Analysedaten aktivieren	Wenn aktiviert, werden Daten über das Verhalten der automatischen Warnmeldungen auf Festplatte gespeichert. Der Standardwert ist **aktiviert**. Die aufbewahrten Daten umfassen den Baselinewert im Laufe der Zeit und den Warnmeldungsverlauf für jede Ereignisquelle. Beachten Sie jedoch, dass Ereignisquellenadresse und -typ anonymisiert sind. Es wird also nur Ihre Ereignisrate angezeigt. Da automatische Warnmeldungen eine Betafunktion ist, sind diese Daten wichtig, um die Wirksamkeit der Funktion zu messen. Dies kann ohne Auswirkung auf die Funktion der automatischen Warnmeldungen deaktiviert werden.
Zurücksetzen	Diese Option verwirft alle ungespeicherten Änderungen für alle Einstellungen auf der Seite.
Anwenden	Klicken Sie auf **Anwenden**, um alle Änderungen an den Werten auf dieser Seite zu speichern.

ESM-Troubleshooting & Anhang

Troubleshooting-Themen:

- Probleme mit Alarmen und Benachrichtigungen
- Mehrfach gesammelte Protokollmeldungen
- Troubleshooting bei Feeds
- Probleme beim Importieren von Dateien
- Negative Policy-Nummerierung

Anhang: Anzeigen von Protokollen von einer Log Decoder-Version vor 11.0

Probleme mit Alarmen und Benachrichtigungen

In diesem Thema wird beschrieben, wie Sie mit möglicherweise auftretenden Problemen mit Alarmen oder Benachrichtigungen umgehen.

Alarme

Wenn Sie Alarme nicht sehen, die Sie erwarten haben, stellen Sie sicher, dass Sie alle erforderlichen Elemente konfiguriert haben, wie unten beschrieben.

Automatische Alarme

Die Option**Automatische Überwachung aktivieren** muss ausgewählt sein, damit automatische Alarme auf dem Bildschirm „Alarme“ angezeigt werden.

Diese Option befindet sich auf der Registerkarte **Einstellungen** (**ADMINISTRATION** > **Ereignisquellen** > **Einstellungen**) und ist standardmäßig ausgewählt. Möglicherweise hat jedoch jemand inzwischen diese Option deaktiviert.

Manuelle Alarme

Alle der folgenden Bedingungen müssen erfüllt sein, damit manuelle Alarme auf dem Bildschirm „Alarme“ angezeigt werden:

- Die Ereignisquelle muss Teil einer Gruppe sein.
- Die Gruppe muss eine Policy haben, in der entweder ein unterer oder ein oberer Schwellenwert (oder beides) definiert wurde.
- Die Gruppenrichtlinie muss aktiviert sein.

Benachrichtigungen

Wenn Alarme angezeigt werden, Sie aber nicht die erwarteten Benachrichtigungen empfangen, vergewissern Sie sich, dass Sie alle erforderlichen Elemente konfiguriert haben, wie unten beschrieben.

Vergewissern Sie sich außerdem, dass Sie die Benachrichtigungsserver und Benachrichtigungsausgaben richtig konfiguriert haben. Ein Großteil der vorläufigen Konfiguration für Benachrichtigungen erfolgt von **ADMINISTRATION > System > Globale Benachrichtigungen** aus. Weitere Informationen finden Sie im Thema **Bereich „Globale Benachrichtigungen“** im *Systemkonfigurationsleitfaden*.

Automatische Benachrichtigungen

Damit das System automatische Benachrichtigungen senden kann, müssen alle der folgenden Bedingungen erfüllt sein:

- Die Option **Automatische Überwachung aktivieren** muss ausgewählt sein (diese Option ist standardmäßig ausgewählt).
- Die Option **Benachrichtigungen von der automatischen Überwachung aktivieren** muss ausgewählt sein. Diese Option ist standardmäßig deaktiviert, daher müssen Sie oder jemand in Ihrem Unternehmen sie aktivieren. Navigieren Sie zu **ADMINISTRATION** > **Ereignisquellen** > **Einstellungen**, um diese Option anzuzeigen.
- Die Ereignisquelle, die den Alarm ausgelöst hat, muss in einer Gruppe sein, die eine Policy aktiviert hat: Beachten Sie, dass keine Schwellenwerte für automatische Benachrichtigungen festgelegt sein müssen.
- Die Policy muss mindestens eine Benachrichtigung konfiguriert haben (entweder E-Mail, SNMP oder Syslog).

Manuelle Benachrichtigungen

Damit das System manuelle Benachrichtigungen senden kann (d. h. eine Benachrichtigung die darauf hinweist, dass ein manueller Alarm ausgelöst wurde):

- Die Ereignisquelle, die den Alarm ausgelöst hat, muss in einer Gruppe sein, die eine Gruppenrichtlinie aktiviert hat.
- Es muss für die Policy ein Schwellenwert festgelegt sein.
- Mindestens eine Benachrichtigung wurde für die Policy konfiguriert.

Mehrfach gesammelte Protokollmeldungen

Unter Umständen kann es vorkommen, dass Meldungen aus derselben Ereignisquelle auf zwei oder mehr Log Collectors gesammelt werden. In diesem Thema wird das Problem beschrieben. Anschließend werden Troubleshooting-Möglichkeiten für das Problem aufgezeigt.

Details

Wenn der ESM-Aggregator identische Ereignisse aus derselben Ereignisquelle auf mehreren Log Collectors findet, erhalten Sie eine Warnmeldung ähnlich der folgenden:

```
2015-03-17 15:25:29,221 [pool-1-thread-6] WARN
com.rsa.smc.esm.groups.events.listeners.EsmStatEventListener -
 192.0.2.21-apache had a previous event only 0 seconds ago; likely because it
exists on multiple log collectors
```

Die Warnmeldung bedeutet, dass die Ereignisquelle `192.0.2.22-apache` auf mehreren Hosts gesammelt wird. Eine Liste dieser Hosts finden Sie auf der Registerkarte **Managen** der Ansicht „Administration > Ereignisquellen“ in der Spalte „Log Collector“.

Bereinigen von mehrfach gesammelten Protokollmeldungen

1. Beenden Sie „collectd“ auf NetWitness Platform und den Log Decoders:

   ```
   Service collectd stop
   ```

2. Entfernen Sie die verbliebene ESM Aggregator-Datei aus NetWitness Platform:

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Setzen Sie den Log Decoder zurück.

   a. Navigieren Sie zum Log Decoder-REST unter `http://<LD_IP_Address>:50102`.

   b. Klicken Sie auf **decoder(*)**, um die Eigenschaften des Decoder anzuzeigen.

   c. Wählen Sie im Drop-down-Menü „Eigenschaften“ die Option **Zurücksetzen** aus und klicken Sie dann auf **Senden**.

4. Wählen Sie auf der Registerkarte „Ereignisquellen verwalten“ im Bereich „Ereignisquellen“ alle Ereignisquellen aus und klicken Sie dann auf −, um sie zu entfernen.

Troubleshooting bei Feeds

Der Zweck des Feedgenerators ist das Erzeugen der Zuordnung einer Ereignisquelle zu einer Gruppenliste, zu der sie gehört.

Wenn es eine Ereignisquelle gibt, aus der Sie Meldungen sammeln, und diese nicht in den korrekten Ereignisquellengruppen angezeigt wird, dann finden Sie in diesem Thema Hintergründe und Informationen, die Ihnen helfen, das Problem zu identifizieren.

Details

Der ESM-Feed ordnet mehrere Schlüssel einem einzigen Wert zu. Er ordnet die Attribute DeviceAddress, Forwarder und DeviceType dem Wert groupName zu.

Der Zweck des ESM-Feeds ist es, die Ereignisquellen-Metadaten mit dem auf dem Log Decoder gesammelten groupName zu versehen.

Funktionsweise

Der Feedgenerator wird planmäßig jede Minute aktualisiert. Er wird jedoch nur ausgelöst, wenn Änderungen (Erstellen, Aktualisieren oder Löschen) in Ereignisquellen oder -gruppen auftreten.

Er erzeugt eine einzige Feeddatei mit Zuordnungen von Ereignisquellen zu Gruppen und verteilt denselben Feed an alle Log Decoder, die mit NetWitness Platform verbunden sind.

Nachdem die Feeddatei auf die Log Decoders hochgeladen wurde, wird den Metadaten für jedes neue Ereignis der groupName hinzugefügt und dieser groupName wird an logstats angehängt.

Sobald der „groupName“ in logstats enthalten ist, gruppiert der ESM-Aggregator Informationen und sendet Sie an ESM. Zu diesem Zeitpunkt sollte in der Registerkarte **Ereignisquellenüberwachung** die Spalte **Gruppenname** angezeigt werden.

Der gesamte Vorgang kann einige Zeit in Anspruch nehmen. Daher kann es nach dem Hinzufügen einer Gruppe oder einer Ereignisquelle einige Sekunden dauern, bevor der Gruppenname angezeigt wird.

Hinweis: Wird das Attribut für die Ereignisquellentyp geändert, wenn der Feed aktualisiert wird, fügt NetWitness Platform einen neuen Eintrag in der „logstats“-Datei hinzu, statt den vorhandenen Eintrag zu ändern. Daher existieren in logdecoder zwei verschiedenen logstats-Einträge. Zuvor vorhandene Meldungen werden unter dem vorherigen Typ aufgeführt und alle neuen Meldungen werden für den neuen Ereignisquellentyp protokolliert.

Feeddatei

Die Feeddatei ist wie folgt formatiert:

```
DeviceAddress, Forwarder, DeviceType, GroupName
```

`DeviceAddress` ist entweder `ipv4, ipv6` oder `hostname`, je nachdem, welcher Typ für die Ereignisquelle definiert wurde.

Im Folgenden ist ein Beispiel der Feeddatei dargestellt:

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apachegr
p"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"
"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","Apach
egrp"
```

Troubleshooting bei Feeds

Sie können die folgenden Elemente überprüfen, um einzugrenzen, wo das Problem auftritt.

10.5 Log Decoders

Sind Ihre NetWitness Platform Log Decoder auf Version 10.5 oder höher aktualisiert? Wenn nicht, müssen Sie ein Upgrade durchführen. In NetWitness Platform Version 10.5 werden Feeds nur an Log Decoder der Version 10.5 gesendet.

Vorhandene Feeddatei

Vergewissern Sie sich, dass das Feed-ZIP-Archiv an folgendem Speicherort vorhanden ist:

`/opt/rsa/sms/esmfeed.zip`

Ändern Sie diese Datei nicht.

Gruppenmetadaten auf LD ausgefüllt

Überprüfen Sie, ob die Gruppenmetadaten auf dem Log Decoder ausgefüllt sind. Navigieren Sie zum Log Decoder-REST und überprüfen Sie die logstats-Datei:

`http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain`

Die ist ein Beispiel für eine logstats-Datei mit Gruppeninformationen:

```
device=apache forwarder=NWAPPLIANCE10304 source=1.2.3.4
count=338 lastSeenTime=2015-Feb-04 22:30:19
lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group,apacheGroup
device=apachetomcat forwarder=NWAPPLIANCE10304
source=5.6.7.8 count=1301 lastSeenTime=2015-Feb-04 22:30:19
lastUpdatedTime=2015-Feb-04 22:30:19
groups=AllOtherGroup,ApacheTomcatGroup
```

Im Text oben sind die Gruppeninformationen fett gedruckt.

Gerätegruppenmetadaten auf dem Concentrator

Vergewissern Sie sich, dass der Metawert **Gerätegruppe** auf dem Concentrator vorhanden ist und dass die Ereignisse Werte für das Feld `device.group` aufweisen.

SMS-Protokolldatei

Überprüfen Sie die SMS-Protokolldatei an dem folgenden Speicherort, um Informations- und Fehlermeldungen anzuzeigen: `/opt/rsa/sms/logs/sms.log`

Im Folgenden finden Sie Beispiele für *Informationsmeldungen*:

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

Im Folgenden finden Sie Beispiele für *Fehlermeldungen*:

```
 Error creating CSV File : <reason>Unable to push the ESM
Feed: Unable to create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> : Error:
<error>
Unable to push the ESM Feed: CSV file is empty, make sure
you have al-least on group with al-least one eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file on
LogDecoder-<logdecoderIP>Unable to push the ESM Feed:
admin@<logdecoderIP>:50002/decoder/parsers received error:
The zip archive
"/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could not
be opened
Unable to push the ESM Feed: <reason>
```

Überprüfen, ob logstats-Daten von ESMReader und ESMAggregator gelesen und weitergeleitet werden

Diese Schritte dienen der Überprüfung, ob die logstats-Daten von **collectd** gesammelt und an das Ereignisquellenmanagement weitergeleitet werden.

ESMReader

1. Fügen Sie auf den Log Decoders in **/etc/collectd.d/NwLogDecoder_ESM.conf** das Flag **debug "true"** hinzu:

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-a2f7-
 ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>
        </stats>
    </Module>
```

```
    <Module "NgEsmReader" "update">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-6737-
4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-a2f7-
 ba7e9a165aae.pem"
        interval  "60"
        query     "update"
        <stats>
        </stats>
    </Module>
</Plugin>
```

2. Führen Sie den folgenden Befehl aus.

   ```
   collectd service restart
   ```

3. Führen Sie den folgenden Befehl aus:

   ```
   tail –f /var/log/messages | grep collectd
   ```

   Vergewissern Sie sich, dass ESMReader die „logstats“ liest und keine Fehler vorhanden sind. Wenn Probleme beim Lesen vorliegen, werden Fehlermeldungen ähnlich der folgenden angezeigt:

   ```
   Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_all:
   error getting ESM data for field "groups" from logstat device=checkpointfw1
   forwarder=PSRTEST source=1.11.51.212. Reason: <reason>Apr 29 18:58:36
   NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_update: error getting
   ESM data for field "forwarder" from logstat device=apachetomcat
   source=10.31.204.240. Reason: <reason>
   ```

ESMAggregator

1. Kommentieren Sie in NetWitness Platform das Flag „verbose“ in **/etc/collectd.d/ESMAggregator.conf** aus:

   ```
   # ESMAggregator module collectd.conf configuration file
   #
   # Copyright (c) 2014 RSA The Security Divsion of EMC
   #
   <Plugin generic_cpp>
   PluginModulePath "/usr/lib64/collectd"
   <Module "ESMAggregator">
           verbose 1
           interval "60"
           cache_save_interval "600"
           persistence_dir "/var/lib/netwitness/collectd"
   </Module>
   </Plugin>
   ```

2. Führen Sie folgenden Befehl aus:

   ```
   collectd service restart.
   ```

3. Führen Sie den folgenden Befehl aus:

   ```
   run "tail –f /var/log/messages | grep ESMA
   ```

   Suchen Sie nach ESMAggregator-Daten und stellen Sie sicher, dass Ihr Logstat-Eintrag in Protokollen verfügbar ist.

Beispielausgabe:

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[0]
logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[1]
logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[2]
groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[3]
logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[4]
utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: Dispatching
ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_counter-3.3.3.3 with a
value of 1752 for NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3
aggregated from 1 log decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[0]
logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[1]
logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[2]
groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[3]
logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: MetaData[4]
utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator: Dispatching
RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_counter-3.3.3.3 with a
value of 1752 for NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3
aggregated from 1 log
```

Konfigurieren des Jobintervalls des JMX-Feedgenerators

Obwohl der Feederzeugungsjob so geplant ist, dass er standardmäßig jede Minute ausgeführt wird, können Sie dies bei Bedarf mit **jconsole** ändern.

So ändern Sie das Jobintervall des Feedgenerators:

1. Öffnen Sie **jconsole** für den SMS-Service.
2. Navigieren Sie in der Registerkarte „MBeans“ zu **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attribute**.
3. Ändern Sie den Wert für die Eigenschaft **FeedGeneratorJobIntervalInMinutes**.
4. Wechseln Sie in derselben Navigationsstruktur zu **Vorgänge** und klicken Sie auf **commit()**. Dadurch wird der neue Wert in der zugehörigen json-Datei unter **/opt/rsa/sms/conf** persistent und der Wert wird verwendet, wenn SMS neu gestartet wird.

Durch das Festlegen eines neuen Wertes wir der Feedgeneratorjob auf das neue Intervall umgeplant.

Probleme beim Importieren von Dateien

Wenn die Importdatei nicht korrekt formatiert ist oder erforderliche Informationen fehlen, wird ein Fehler angezeigt und die Datei wird nicht importiert.

Überprüfen Sie Folgendes:

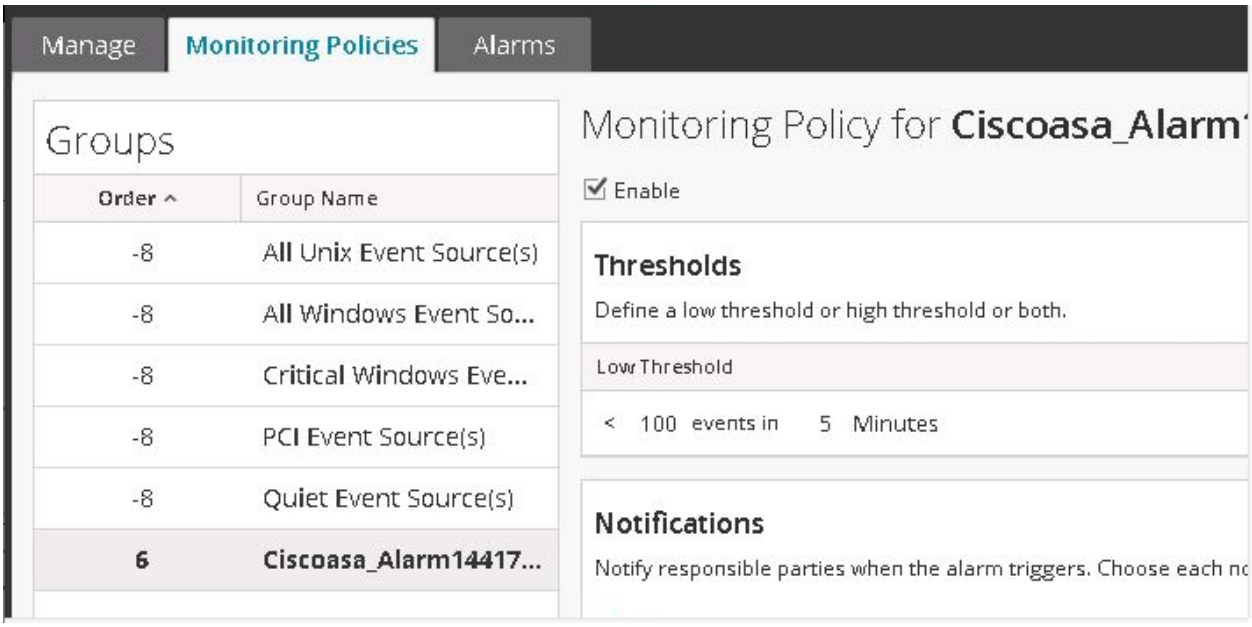
- Wenn Sie unbekannte Quellen hinzufügen, muss jede Zeile in der Datei eine Kombination der erforderlichen Attribute enthalten:
  - IP, IPv6 oder Hostname und
  - Ereignisquelltyp
- Die erste Zeile der Datei muss Header-Namen enthalten, die mit den Namen in NetWitness Platform übereinstimmen. Sie können eine einzelne Ereignisquelle exportieren, um eine Liste der korrekten Header-Namen zu erhalten. Betrachten Sie die exportierte CSV-Datei: die erste Zeile der Datei enthält den korrekten Satz Attribute/Spaltennamen.

Negative Policy-Nummerierung

Möglicherweise sehen Sie negative Zahlen im Feld „Reihenfolge“ im Bereich „Gruppen“ auf der Registerkarte „Policies überwachen“. Dieses Thema beschreibt einen Workaround, um das richtige Nummerierungsschema für Ihre Policies wiederherzustellen.

Details

Der folgende Bildschirm zeigt ein Beispiel für die Situation, in der die Nummern der Gruppen-Policies negativ sind.



Wenn Sie auf diese Situation treffen, ziehen Sie per Drag-and-drop die oberste Gruppe (**Alle Unix-Ereignisquellen** im obigen Bild) auf die Position hinter der letzten Gruppe (**Ciscoasa_Alarm14417**). Dadurch wird die normale Nummerierung wiederhergestellt. Sie können dann weiterhin per Drag-and-drop Gruppen verschieben, bis sie in der richtigen Reihenfolge für Ihr Unternehmen stehen.

Bereinigen von mehrfach gesammelten Protokollmeldungen

1. Beenden Sie „collectd“ auf NetWitness Platform und den Log Decoders:

   ```
   Service collectd stop
   ```

2. Entfernen Sie die verbliebene ESM Aggregator-Datei aus NetWitness Platform:

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Setzen Sie den Log Decoder zurück.

   a. Navigieren Sie zum Log Decoder-REST unter `http://<LD_IP_Address>:50102`.

   b. Klicken Sie auf **decoder(*)**, um die Eigenschaften des Decoder anzuzeigen.

   c. Wählen Sie im Drop-down-Menü „Eigenschaften“ die Option **Zurücksetzen** aus und klicken Sie dann auf **Senden**.

4. Wählen Sie auf der Registerkarte „Ereignisquellen verwalten“ im Bereich „Ereignisquellen“ alle Ereignisquellen aus und klicken Sie dann auf −, um sie zu entfernen.

Anzeigen von Protokollen von einer Log Decoder-Version vor 11.0

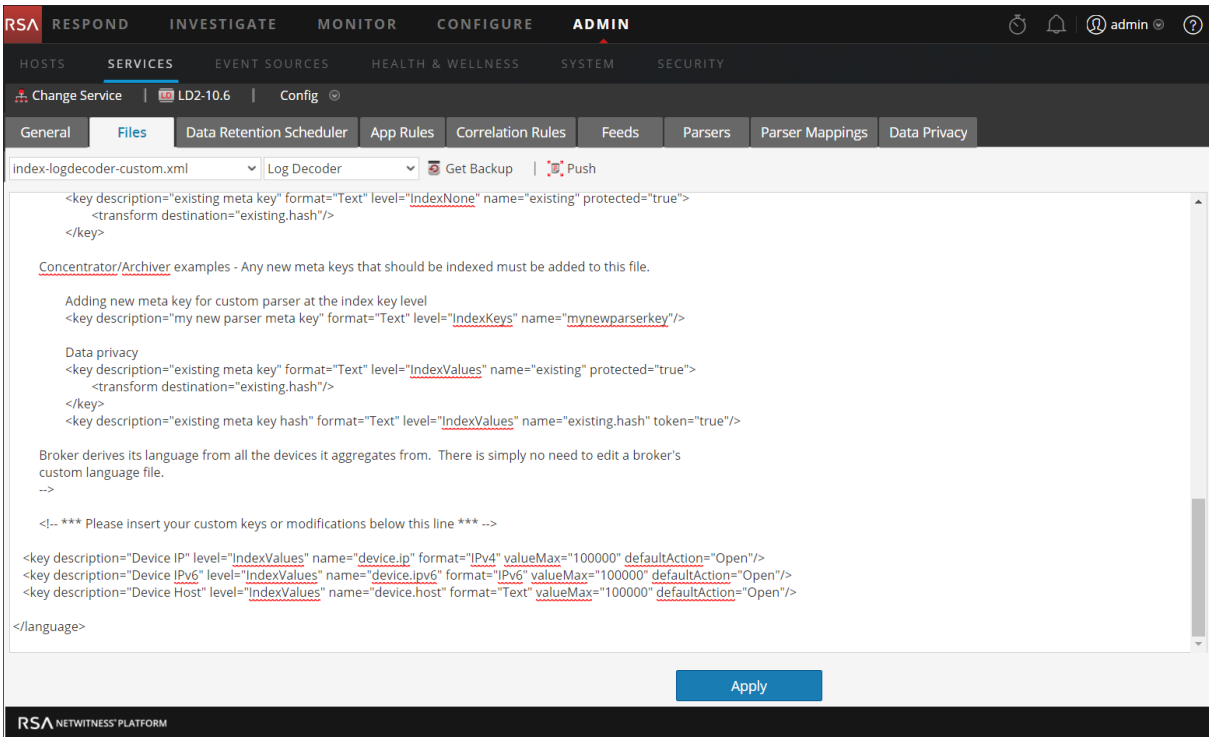
In RSA NetWitness® Platform 11.0. besteht nun die Möglichkeit, eine kleine Auswahl der letzten Protokolle für bestimmte Geräte auf den jeweiligen Detail-Registerkarten der Ansicht „Erkennung“ anzuzeigen. Standardmäßig besitzen Log Decoder vor Version 11.0 nicht die erforderliche Konfiguration zum Aktivieren dieser Funktion. Dies ist jedoch durch Vornehmen einiger geringfügiger Änderungen möglich.

Um die Protokollvorschau für eine Log Decoder-Version vor 11.0.0.0 zu aktivieren, führen Sie auf dem Log Decoder die folgenden Schritte aus:

1. Navigieren Sie zu **ADMIN > Services**, wählen Sie einen Log Decoder aus und klicken Sie dann auf **> Ansicht > Konfiguration**.
2. Klicken Sie auf die Registerkarte **Dateien** und wählen Sie aus dem Drop-down-Menü **index-logdecoder-custom.xml** aus.
3. Fügen Sie die folgenden drei Zeilen am Ende der Datei hinzu (vor dem schließenden Sprachtag):

```
<key description="Device IP" level="IndexValues" name="device.ip" format="IPv4" valueMax="100000"
defaultAction="Open"/>
<key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
valueMax="100000" defaultAction="Open"/>
<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```

4. Klicken Sie auf **Anwenden**.



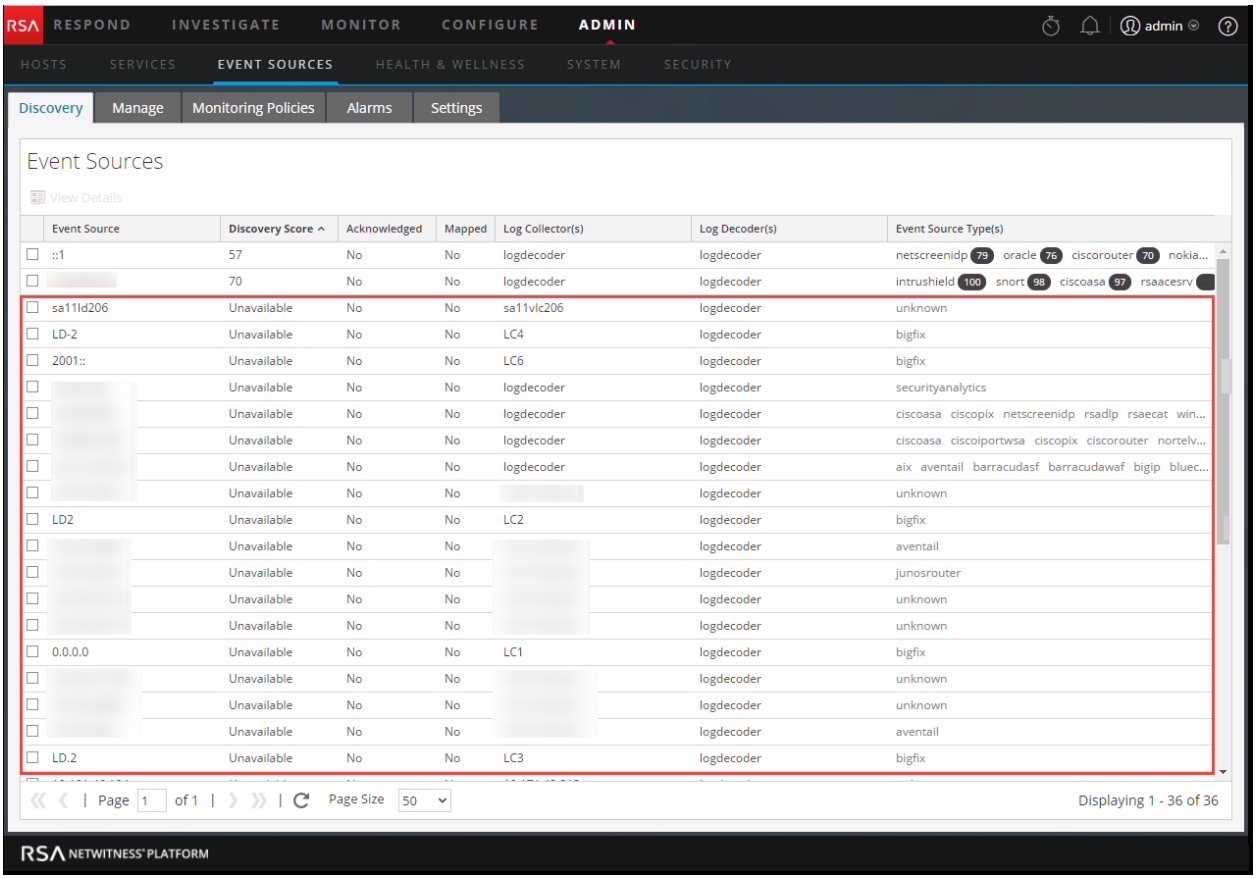
5. Starten Sie den Log Decoder folgendermaßen neu.

   Wählen Sie **Log Decoder > Durchsuchen > Sys > Eigenschaften > Herunterfahren** aus.

Dies ist ein Beispiel der Datei **index-logdecoder-custom.xml**.

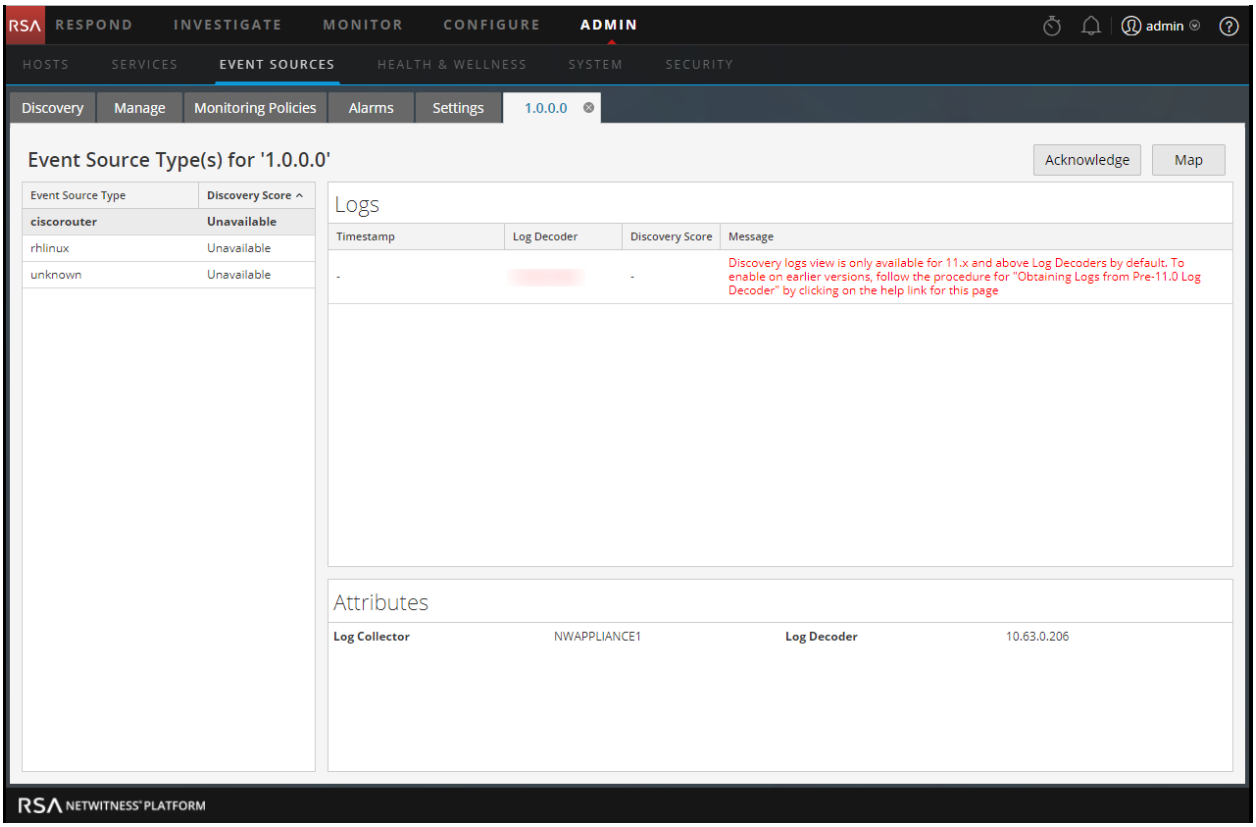
Hinweis: Discovery Scores sind nur für Log Decoder ab Version 11.0 verfügbar. Discovery Scores für eine Log Decoder-Version vor 11.0 werden als „Nicht verfügbar“ angezeigt.

Das folgende Beispiel zeigt den Discovery Score für eine Log Decoder-Version vor 11.0 in der Ansicht **Details** als **Nicht verfügbar** an.



Hinweis: Geräteprotokolle sind nur für Log Decoder ab Version 11.0 verfügbar.

Das folgende Beispiel zeigt die Meldung, die im Protokollbereich für eine Log Decoder-Version vor 11.0 angezeigt wird.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Discovery
Manage
Monitoring Policies
Alarms
Settings
1.0.0.0
Event Source Type(s) for '1.0.0.0'
Acknowledge
Map
Event Source Type
Discovery Score
ciscorouter
Unavailable
rhlinux
Unavailable
unknown
Unavailable
Logs
Timestamp
Log Decoder
Discovery Score
Message
Discovery logs view is only available for 11.x and above Log Decoders by default. To enable on earlier versions, follow the procedure for "Obtaining Logs from Pre-11.0 Log Decoder" by clicking on the help link for this page
Attributes
Log Collector
NWAPPLIANCE1
Log Decoder
10.63.0.206
RSA NETWITNESS PLATFORM